**به نام خدا**

# پروفایل حفاظتی

## سامانه مدیریت یکپارچه تهدیدات

## (UTM)

اسفند ۹۶

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 را که در این سند برای برآورده کردن الزامات ارائه‌شده‌اند در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را در راستای این اهداف تهیه کرده است. این سند معرفی‌کننده‌ی الزامات کارکرد امنیتی برای سیستم مدیریت یکپارچه تهدیدات است تا تولیدکنندگان این محصول بتوانند بر مبنای این سند کارکردهای امنیتی را در محصول خود لحاظ کنند و همچنین سند هدف امنیتی آن را ارائه دهند. در بخش اول به معرفی سیستم مدیریت یکپارچه تهدیدات پرداخته‌شده است. سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدات، اجرای خط‌مشی‌ها و به‌کار 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 محصول UTM در این سند مطرح‌شده است، عبارت‌اند از:

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

هریک از این کلاس‌ها، از مجموعه‌ای از خانواده‌ها تشکیل شده 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 می‌کند.

فهرست

۱ شرح محصول UTM ..... ۸
۱,۱ موارد کاربرد محصول ..... ۸
۲ تعریف مسائل امنیتی ..... ۹
۲,۱ تهدیدات ..... ۱۰
۲,۱,۱ ارتباط با دستگاه‌های شبکه ..... ۱۰
۲,۱,۲ به‌روزرسانی‌های معتبر ..... ۱۳
۲,۱,۳ فعالیت ممیزی‌شده ..... ۱۴
۲,۱,۴ داده‌ها و اطلاعات محرمانه دستگاه و سرپرست ..... ۱۵
۲,۱,۵ از کار افتادن کارکردهای امنیتی دستگاه ..... ۱۷
۲,۲ فرضیات ..... ۱۷
۲,۲,۱ حفاظت فیزیکی ..... ۱۸
۲,۲,۲ کارکرد محدود ..... ۱۸
۲,۲,۳ عدم محافظت از ترافیک ..... ۱۸
۲,۲,۴ سرپرست مورد اعتماد ..... ۱۸
۲,۲,۵ به‌روزرسانی منظم ..... ۱۹
۲,۲,۶ امنیت اطلاعات محرمانه سرپرست ..... ۱۹
۲,۲,۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده) ..... ۱۹
۲,۲,۸ اطلاعات باقیمانده ..... ۱۹
۲,۳ خط‌مشی امنیتی سازمان ..... ۱۹
۲,۳,۱ بنر دسترسی ..... ۱۹
۳ اهداف امنیتی. ..... ۲۰

۳,۱ اهداف امنیتی مربوط به محیط عملیاتی ..... ۲۰
۳,۱,۱ امنیت فیزیکی ..... ۲۰
۳,۱,۲ عدم کارکرد عمومی ..... ۲۰
۳,۱,۳ محافظت از ترافیک ..... ۲۰
۳,۱,۴ سرپرست مورد اعتماد ..... ۲۰
۳,۱,۵ به‌روزرسانی ..... ۲۰
۳,۱,۶ امنیت حساب کاربری سرپرست ..... ۲۰
۳,۱,۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده) ..... ۲۱
۳,۱,۸ اطلاعات باقیمانده ..... ۲۱
۴ الزامات کارکرد امنیتی ..... ۲۱
۴,۱ کلاس ممیزی امنیت ..... ۳۰
۴,۲ پشتیبانی رمزنگاری (FCS) ..... ۳۸
۴,۳ الزامات پروتکل IPsec ..... ۴۴
4.4 کلاس دیواره آتش (FFW) ..... ۵۱
۴,۵ کلاس شناسایی و احراز هویت ..... ۵۶
۴,۶ کلاس مدیریت امنیت ..... ۶۰
۴,۷ کلاس حفاظت از محصول مورد ارزیابی ..... ۶۵
۴,۷,۱ آزمون محصول مورد ارزیابی ..... ۶۶
۴,۷,۲ به‌روزرسانی امن ..... ۶۷
۴,۸ دسترسی به محصول ..... ۷۲
4.9 کلاس کانال‌ها/مسیرهای مورد اعتماد ..... ۷۳
۴,۱۰ کلاس IPS: جلوگیری از نفوذ ..... ۷۵

5 الزامات تضمین امنیت ..... ۸۳
5.1 کلاس توسعه..... ۸۳
5.1.1 مشخصات کارکردی..... ۸۴
5.2 کلاس راهنمای کاربر..... ۸۶
۵,۲,۱ راهنمای کاربردی ..... ۸۷
۵,۲,۲ راهنمای آماده‌سازی ..... ۸۹
5.3 کلاس آزمون..... ۹۰
5.3.1 آزمون مستقل ..... ۹۱
5.4 کلاس آسیب‌پذیری..... ۹۲
۵,۴,۱ تحلیل آسیب‌پذیری..... ۹۲
5.5 کلاس پشتیبانی از چرخه حیات..... ۹۳
5.5.1 قابلیت‌های پیکربندی..... ۹۳
۵,۵,۲ حوزه پیکربندی ..... ۹۵
۶ پیوست یک: الزامات اختیاری ..... ۹۶
۶,۱ کلاس ممیزی امنیت..... ۹۶
۶,۲ کلاس شناسایی و احراز هویت..... ۱۰۰
۶,۳ کلاس مدیریت امنیت..... ۱۰۱
۶,۴ کلاس حفاظت از محصول مورد ارزیابی ..... ۱۰۳
۶,۵ کلاس ارتباطات..... ۱۰۴
۶,۶ الزامات محافظت از هدف ارزیابی..... ۱۰۵
۶,۷ الزامات تخصیص منابع..... ۱۰۵
۶,۸ کلاس دیواره آتش (FFW)..... ۱۰۶

۶,۹ الزامات IPS: جلوگیری از نفوذ ..... ۱۰۷
۷ پیوست دو: الزامات مبتنی بر انتخاب ..... ۱۰۸
7.1 الزامات پروتکل DTLS Client ..... ۱۱۰
۷,۲ الزامات پروتکل DTLS Clint /احراز هویت ..... ۱۱۳
7.3 الزامات پروتکل DTLS Server ..... ۱۱۷
۷,۴ الزامات پروتکل DTLS Server /احراز هویت دوطرفه ..... ۱۲۰
۷,۵ الزامات پروتکل HTTPS ..... ۱۲۴
۷,۶ الزامات پروتکل SSH Client ..... ۱۲۵
۷,۷ الزامات پروتکل SSH Server ..... ۱۲۸
۷,۸ الزامات پروتکل TLS Client ..... ۱۳۰
7.9 الزامات پروتکل TLS Client/ احراز هویت ..... ۱۳۳
۷,۱۰ الزامات پروتکل TLS Server ..... ۱۳۷
۷,۱۱ الزامات پروتکل TLS Server/ احراز هویت دوطرفه ..... ۱۳۹
۷,۱۲ الزامات شناسایی و احراز هویت ..... ۱۴۲
۷,۱۳ الزامات خودآزمایی محصول مورد ارزیابی ..... ۱۴۵
۷,۱۴ الزامات به‌روزرسانی امن ..... ۱۴۷
۸ تعاریف ..... ۱۴۸
۸,۱ تعریف حملات ..... ۱۴۸
۸,۲ تعریف عبارات و مخفف‌ها ..... ۱۵۰
۹ مراجع ..... ۱۵۱

# ۱ شرح محصول UTM

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

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

از آنجایی که UTM یک تجهیز شبکه است بنابراین برآورده شدن تمامی الزامات پروفایل تجهیز شبکه برای محصول UTM اجباری است و در این پروفایل گنجانده شده است.

## ۱,۱ موارد کاربرد محصول

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

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

علاوه بر آنکه پیاده‌سازی، مدیریت و به‌روزرسانی سیستم‌های مختلف امنیتی مشکل است، این پیاده‌سازی، مدیریت و به‌روزرسانی باعث افزایش پیچیدگی عملیات و هزینه‌های بالاسری نیز می‌شود. بدین ترتیب سازمان‌ها امروزه از یک نگرش یکپارچه برای امنیت و بهره‌وری شبکه استفاده می‌کنند که فنّاوری‌های قدیمی مجزا را ترکیب کرده و به صورت یک جا آن‌ها را مدیریت می‌کنند.

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

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

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

## ۲ تعریف مسائل امنیتی

هر محصول UTM برای ایفای یک نقش در زیرساخت شبکه طراحی شده است. به منظور ایفای این نقش، دستگاه مذکور ارتباطاتی را از طریق شبکه با دیگر دستگاه‌های شبکه و سایر موجودیت‌های شبکه (موجودیتی که به عنوان یک دستگاه شبکه تعریف نشده است) برقرار می‌کند. در عین حال، محصول UTM باید مجموعه‌ای از حداقل کارکرد امنیتی مشترک[۱] که از همه دستگاه‌های شبکه انتظار می‌رود را ارائه کند. حداقل کارکرد امنیتی مشترک برای مقابله با تهدیدات مشترک پیش روی دستگاه‌های شبکه، مسئله امنیتی است که یک محصول UTM مطابق با پروفایل حاضر باید به آن بپردازد. این تهدیدات در مقابل تهدیداتی قرار می‌گیرند که یک کارکرد خاص از یک نوع خاص از دستگاه شبکه را هدف قرار می‌دهند. مجموعه حداقل کارکرد امنیتی مشترک باید قابلیت‌های زیر را داشته باشند:

- برقراری ارتباط با دستگاه‌های مجاز و غیرمجاز شبکه
- توانایی انجام به‌روزرسانی‌های معتبر و امن
- توانایی ممیزی فعالیت‌های دستگاه‌ها
- توانایی ذخیره‌سازی و استفاده امن از داده‌ها و اطلاعات محرمانه سرپرست و دستگاه

[۱] Common security functionality

- توانایی انجام خودآزمایی برای از کار افتادن مؤلفه‌های حیاتی دستگاه.

## ۲,۱ تهدیدات

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

### ۲,۱,۱ ارتباط با دستگاه‌های شبکه

یک محصول UTM با سایر دستگاه‌های شبکه و موجودیت‌های شبکه ارتباط برقرار می‌کند. مقصد این ارتباط ممکن است از لحاظ منطقی یا جغرافیایی یک دستگاه راه دور به شمار آید و مسیر ارتباط ممکن است از سیستم‌های متعدد دیگری بگذرد. این احتمال وجود دارد که سیستم‌های میانی مورد اعتماد نباشند و ارتباط غیرمجازی را با محصول UTM برقرار کنند یا ارتباطات مجاز را در معرض خطر قرار دهند. کارکرد امنیتی محصول UTM باید این قابلیت را داشته باشد که از ترافیک حساس شبکه (مانند ترافیک سرپرستی، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست) محافظت کند. ارتباطات برقرارشده با محصول UTM را می‌توان به دو دسته تقسیم‌بندی کرد: ارتباطات مجاز و ارتباطات غیرمجاز.

ارتباطات مجاز شامل ترافیکی است که بر اساس خط‌مشی محصول UTM، اجازه جریان یافتن دارد. ارتباطات مجاز ترافیک حساس شبکه را شامل می‌شود که از آن جمله می‌توان به ترافیک سرپرستی محصول UTM و ارتباطات آن با یک سرور ممیزی یا احراز هویت اشاره کرد. حفاظت از این ارتباطات نیازمند استفاده از یک کانال امن است. کارکرد امنیتی محصول UTM باید به گونه‌ای باشد که اطمینان حاصل کند تنها ارتباطات مجاز می‌توانند برقرار شوند. این کارکرد امنیتی باید کانال امنی را برای جریان یافتن ترافیک حساس شبکه فراهم آورد. تمامی ارتباطات دیگر، ارتباطات غیرمجاز به شمار می‌آیند.

تهدید اصلی علیه ارتباطات محصول UTM که در این پروفایل حفاظتی به آن پرداخته می‌شود، یک موجودیت غیرمجاز خارجی است که تلاش می‌کند به ترافیک حساس شبکه دسترسی پیدا کند، آن را تغییر دهد یا به هر طریقی آن را افشا کند. در صورتی که از الگوریتم‌های رمزنگاری نامناسبی استفاده شده باشد یا پروتکل‌های تونل‌زنی غیراستاندارد و اطلاعات محرمانه سرپرستی ضعیفی به کار گرفته شده باشند، یک عامل تهدید می‌تواند به صورت غیرمجاز به دستگاه دسترسی پیدا کند. استفاده از رمزنگاری ضعیف یا عدم استفاده از چنین الگوریتمی به طور کل، باعث می‌شود که عامل تهدید بتواند با کمترین تلاش، ترافیک را بخواند، دست‌کاری کند یا کنترل

کند. استفاده از پروتکل‌های تونل‌زنی غیراستاندارد نه تنها قابلیت هم‌کنش‌پذیری[۱] دستگاه را محدود می‌کند، بلکه ضمانت و اعتماد حاصل از استانداردسازی را نیز از دستگاه می‌گیرد.

#### ۲٫۱٫۱٫۱ دسترسی سرپرستی غیرمجاز

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

منطق الزام کارکرد امنیتی (SFR):

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

[۱] Interoperability

#### ۲,۱,۱,۲ رمزنگاری ضعیف

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

منطق الزام کارکرد امنیتی:

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

#### ۲,۱,۱,۳ کانال‌های ارتباطی غیرقابل‌اعتماد

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

منطق الزام کارکرد امنیتی:

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

---

[۱] Cryptographic exhaust

[۲] Brute force

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

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

#### ۲,۱,۱,۴ نقاط پایانی با احراز هویت ضعیف

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

منطق الزام کارکرد امنیتی:

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

### ۲,۱,۲ به‌روزرسانی‌های معتبر

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

نسخه‌های به‌روزنشده نرم‌افزارها یا ثابت‌افزارها می‌توانند محصول UTM را در معرض خطر عوامل تهدیدی قرار دهند که در پی سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده آن‌ها هستند. به‌روزرسانی‌های تأیید نشده یا

به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تائید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روزشده را در معرض خطر عوامل تهدیدی قرار می‌دهند که به دنبال بهره‌گیری از نرم‌افزار یا ثابت‌افزار برای رسیدن به مقاصد خویش هستند.

#### ۲,۱,۲,۱ به‌روزرسانی‌های مخرب

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

منطق الزام کارکرد امنیتی:

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

### ۲,۱,۳ فعالیت ممیزی‌شده

سرپرستان می‌توانند با ممیزی فعالیت‌های محصول UTM، وضعیت دستگاه را به خوبی پایش کنند. این فرایند امکان بررسی، گزارش‌دهی در خصوص کارکردهای امنیتی، بازسازی رویدادها و تحلیل مشکل امنیتی را برای سرپرست فراهم می‌آورد. پردازش‌هایی که در پاسخ به فعالیت‌های دستگاه انجام می‌شوند، نشانه‌هایی از به خطر افتادن یا از کار افتادن کارکردهای امنیتی را ارائه می‌کنند. در صورتی که فعالیت‌هایی انجام شده و بر کارکرد امنیتی تأثیر گذاشته باشند اما نشانه‌ای دال بر انجام شدن آن‌ها تولید و پایش نشده باشد، ممکن است که این فعالیت‌ها بدون آگاهی سرپرست صورت گرفته باشند. علاوه بر این، در صورتی که سوابق تولید و نگهداری نشده باشند، امکان بازسازی شبکه و درک شدت و میزان آسیب‌های وارده تحت تأثیر قرار خواهد گرفت. داده‌های ممیزی ثبت‌شده در خصوص تغییر و حذف غیرمجاز، باید به دقت محافظت شوند. داده‌های مذکور ممکن است در درون محصول یا در هنگام انتقال به حافظه‌های خارجی مورد حمله قرار گیرند.

توجه داشته باشید که بر اساس این پروفایل حفاظتی مشارکتی، محصول UTM باید داده‌های ممیزی را تولید کند و قابلیت ارسال آن‌ها به یک موجودیت شبکه مورد اعتماد (مثال؛ سرور syslog) را داشته باشد.

#### ۲,۱,۳,۱ فعالیت ردیابی‌نشده

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

منطق الزام کارکرد امنیتی:

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

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

محصول UTM دربردارنده داده‌ها و اطلاعات محرمانه‌ای است که باید به طور امن ذخیره‌سازی شوند و امکان دسترسی به آن‌ها تنها برای موجودیت‌های مجاز وجود داشته باشد. به عنوان مثال، می‌توان به اطلاعات محرمانه احراز هویت و پیکربندی نرم‌افزار و ثابت‌افزار و اطلاعات محرمانه سرپرستی اشاره کرد. کلیدهای سرپرست و دستگاه، اطلاعات کلید و اطلاعات محرمانه احراز هویت را باید در برابر دست‌کاری و افشای غیرمجاز محافظت کرد. علاوه بر این، کارکرد امنیتی دستگاه باید تغییر اطلاعات محرمانه پیش‌فرض احراز هویت را (مانند؛ کلمه‌های عبور سرپرست) ملزم کند.

عدم ذخیره‌سازی امن و مدیریت نامناسب داده‌ها و اطلاعات محرمانه مانند؛ رمزگذاری نکردن اطلاعات محرمانه درون فایل‌های پیکربندی یا دسترسی به کلیدهای نشست کانال امن، به مهاجم امکان می‌دهد تا به محصول UTM دسترسی پیدا کند و حتی امنیت شبکه را از طریق دست‌کاری ظاهراً مجاز پیکربندی یا ترتیب دادن حملات کسی در میانه در معرض خطر قرار دهد. این حملات به موجودیت غیرمجاز امکان می‌دهند تا با استفاده از اطلاعات محرمانه سرپرست امنیتی، به کارکردهای سرپرستی دست پیدا کند و آن‌ها را اجرا کند و همچنین به عنوان یک دستگاه پایانی مجاز، تمامی ترافیک را دریافت کند. بدین ترتیب، شناسایی حملات امنیتی و بازسازی شبکه دشوار خواهد شد و حتی دسترسی غیرمجاز مهاجم به داده‌های دستگاه و سرپرست ادامه خواهد یافت.

#### ۲,۱,۴,۱ به خطر افتادن کارکرد امنیتی

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

منطق الزام کارکرد امنیتی:

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

#### ۲,۱,۴,۲ هک شدن گذرواژه

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

منطق الزام کارکرد امنیتی:

- الزامات طول‌های گذرواژه و کاراکترهای موجود در آن، در FIA_PMG_EXT.1 مشخص شده است.

- حفاظت از ورود گذرواژه از طریق بازخورد مبهم در FIA_UAU.7 مشخص شده است.
- اقدامات به دست آوردن تعداد حد آستانه شکست‌های متوالی گذرواژه در FIA_AFL.1 مشخص شده است.
- الزامات ذخیره‌سازی امن گذرواژه‌ها در FPT_APW_EXT.1 مشخص شده است.

### ۲,۱,۵ از کار افتادن کارکردهای امنیتی دستگاه

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

#### *۲,۱,۵,۱ از کار افتادن کارکرد امنیتی*

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

منطق الزام کارکرد امنیتی:

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

## ۲,۲ فرضیات

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

[۱] Roots of trust

### ۲,۲,۱ حفاظت فیزیکی

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

### ۲,۲,۲ کارکرد محدود

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

### ۲,۲,۳ عدم محافظت از ترافیک

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

### ۲,۲,۴ سرپرست مورد اعتماد

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

### ۲,۲,۵ به‌روزرسانی منظم

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

### ۲,۲,۶ امنیت اطلاعات محرمانه سرپرست

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

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

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

### ۲,۲,۸ اطلاعات باقیمانده

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

## ۲,۳ خط‌مشی امنیتی سازمان

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

### ۲,۳,۱ بنر دسترسی

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

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

# ۳ اهداف امنیتی

## ۳,۱ اهداف امنیتی مربوط به محیط عملیاتی

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

### ۳,۱,۱ امنیت فیزیکی

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

### ۳,۱,۲ عدم کارکرد عمومی

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

### ۳,۱,۳ محافظت از ترافیک

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

### ۳,۱,۴ سرپرست مورد اعتماد

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

### ۳,۱,۵ به‌روزرسانی

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

### ۳,۱,۶ امنیت حساب کاربری سرپرست

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

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

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

### ۳,۱,۸ اطلاعات باقیمانده

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

## ۴ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول ۴-۱ هستند و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول ۴-۱ آمده‌اند. الزامات تشریح شده در این بخش الزامی هستند و تمامی محصولات باید آن‌ها را رعایت کنند. بر اساس انتخاب‌هایی که در این الزامات صورت می‌گیرند، لازم خواهد بود که برخی الزامات مورداشاره در پیوست دو نیز رعایت شوند. برخی الزامات اختیاری نیز ممکن است از پیوست یک برگزیده شوند. موارد ذکرشده در قالب فعالیت‌های ارزیابی، بیان می‌کنند که توسعه‌دهندگان محصول مورد ارزیابی باید چه مواردی را رعایت کنند.

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

*جدول ۴-۱ الزامات کارکرد امنیتی*

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۱ | تولید داده ممیزی ۱ | FAU_GEN.1.1 |
| ۲ | تولید داده ممیزی ۲ | FAU_GEN.1.2 |
| ۳ | تولید داده ممیزی ۳ | FAU_GEN.2.1 |
| ۴ | محل ذخیره‌سازی داده‌های ممیزی ۱ | FAU_STG_EXT.1.1 |
| ۵ | محل ذخیره‌سازی داده‌های ممیزی ۲ | FAU_STG_EXT.1.2 |
| ۶ | محل ذخیره‌سازی داده‌های ممیزی ۳ | FAU_STG_EXT.1.3 |
| 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 | الزامات پروتکل IPSEC (۱) | FCS_IPSEC_EXT.1.1 |
| ۱۷ | الزامات پروتکل IPSEC (۲) | FCS_IPSEC_EXT.1.2 |
| ۱۸ | الزامات پروتکل IPSEC (۳) | FCS_IPSEC_EXT.1.3 |
| ۱۹ | الزامات پروتکل IPSEC (۴) | FCS_IPSEC_EXT.1.4 |
| ۲۰ | الزامات پروتکل IPSEC (۵) | FCS_IPSEC_EXT.1.5 |
| ۲۱ | الزامات پروتکل IPSEC (۶) | FCS_IPSEC_EXT.1.6 |
| ۲۲ | الزامات پروتکل IPSEC (۷) | FCS_IPSEC_EXT.1.7 |
| ۲۳ | الزامات پروتکل IPSEC (۸) | FCS_IPSEC_EXT.1.8 |
| ۲۴ | الزامات پروتکل IPSEC (۹) | FCS_IPSEC_EXT.1.9 |
| ۲۵ | الزامات پروتکل IPSEC (۱۰) | FCS_IPSEC_EXT.1.10 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۲۶ | الزامات پروتکل IPSEC (۱۱) | FCS_IPSEC_EXT.1.11 |
| ۲۷ | الزامات پروتکل IPSEC (۱۲) | FCS_IPSEC_EXT.1.12 |
| ۲۸ | الزامات پروتکل IPSEC (۱۳) | FCS_IPSEC_EXT.1.13 |
| ۲۹ | الزامات پروتکل IPSEC (۱۴) | FCS_IPSEC_EXT.1.14 |
| ۳۰ | فیلترینگ حالتمند ۱ | FFW_RUL_EXT.1.1 |
| ۳۱ | فیلترینگ حالتمند ۲ | FFW_RUL_EXT.1.2 |
| ۳۲ | فیلترینگ حالتمند ۳ | FFW_RUL_EXT.1.3 |
| ۳۳ | فیلترینگ حالتمند ۴ | FFW_RUL_EXT.1.4 |
| ۳۴ | فیلترینگ حالتمند ۵ | FFW_RUL_EXT.1.5 |
| ۳۵ | فیلترینگ حالتمند ۶ | FFW_RUL_EXT.1.6 |
| ۳۶ | فیلترینگ حالتمند ۷ | FFW_RUL_EXT.1.7 |
| ۳۷ | فیلترینگ حالتمند ۸ | FFW_RUL_EXT.1.8 |
| ۳۸ | فیلترینگ حالتمند ۹ | FFW_RUL_EXT.1.9 |
| ۳۹ | فیلترینگ حالتمند ۱۰ | FFW_RUL_EXT.1.10 |
| ۴۰ | مدیریت احراز هویت ناموفق ۱ | FIA_AFL.1.1 |
| ۴۱ | مدیریت احراز هویت ناموفق ۲ | FIA_AFL.1.2 |
| ۴۲ | مدیریت رمز عبور ۱ | FIA_PMG_EXT.1.1 |
| ۴۳ | شناسایی و احراز هویت کاربر ۱ | FIA_UIA_EXT.1.1 |
| ۴۴ | شناسایی و احراز هویت کاربر ۲ | FIA_UIA_EXT.1.2 |
| ۴۵ | سازوکار احراز هویت بر اساس رمز عبور ۲ | FIA_UAU_EXT.2.1 |
| ۴۶ | احراز هویت کاربر ۱۰ | FIA_UAU.7.1 |
| ۴۷ | مدیریت کارکرد در محصول IPS۱ | FMT_SMF.1.1 |
| ۴۸ | مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن | FMT_MOF.1.1(1)/TrustedUpdate |
| ۴۹ | مدیریت داده‌های محصول ۱ | FMT_MTD.1.1 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۵۰ | کارکرد مدیریتی محصول ۱ | FMT_SMF.1.1 |
| ۵۱ | نقش‌های امنیتی ۳ | FMT_SMR.2.1 |
| ۵۲ | نقش‌های امنیتی ۴ | FMT_SMR.2.2 |
| ۵۳ | نقش‌های امنیتی ۵ | FMT_SMR.2.3 |
| ۵۴ | محافظت از داده‌های محصول (کلیدهای متقارن) ۱ | FPT_SKP_EXT.1.1 |
| ۵۵ | حفاظت از گذرواژه سرپرست محصول ۱ | FPT_APW_EXT.1.1 |
| ۵۶ | حفاظت از گذرواژه سرپرست محصول ۲ | FPT_APW_EXT.1.2 |
| ۵۷ | خودآزمایی محصول ۱ | FPT_TST_EXT.1.1 |
| ۵۸ | به‌روزرسانی امن ۱ | FPT_TUD_EXT.1.1 |
| ۵۹ | به‌روزرسانی امن ۲ | FPT_TUD_EXT.1.2 |
| ۶۰ | به‌روزرسانی امن ۳ | FPT_TUD_EXT.1.3 |
| ۶۱ | مهرهای زمانی ۱ | FPT_STM_EXT.1.1 |
| ۶۲ | مهرهای زمانی ۲ | FPT_STM_EXT.1.2 |
| ۶۳ | قفل‌کردن و خاتمه دادن به نشست‌ها ۷ | FTA_SSL_EXT.1.1 |
| ۶۴ | قفل‌کردن و خاتمه دادن به نشست‌ها ۵ | FTA_SSL.3.1 |
| ۶۵ | قفل‌کردن و خاتمه دادن به نشست‌ها ۶ | FTA_SSL.4.1 |
| ۶۶ | پیغام‌های هشدار در رابطه با استفاده محصول ۱ | FTA_TAB.1.1 |
| ۶۷ | کانال امن ۱ | FTP_ITC.1.1 |
| ۶۸ | کانال امن ۲ | FTP_ITC.1.2 |
| ۶۹ | کانال امن ۳ | FTP_ITC.1.3 |
| ۷۰ | مسیر امن ۱ | FTP_TRP.1.1 |
| ۷۱ | مسیر امن ۲ | FTP_TRP.1.2 |
| ۷۲ | مسیر امن ۳ | FTP_TRP.1.3 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۷۳ | کارکرد IPS مبتنی بر رفتار غیرعادی ۱ | IPS_ABD_EXT.1.1 |
| ۷۴ | کارکرد IPS مبتنی بر رفتار غیرعادی ۲ | IPS_ABD_EXT.1.2 |
| ۷۵ | کارکرد IPS مبتنی بر رفتار غیرعادی ۳ | IPS_ABD_EXT.1.3 |
| ۷۶ | بلوکه کردن آدرس IP ۱ | IPS_IPB_EXT.1.1 |
| ۷۷ | بلوکه کردن آدرس IP ۲ | IPS_IPB_EXT.1.2 |
| ۷۸ | تحلیل ترافیک شبکه ۱ | IPS_NTA_EXT.1.1 |
| ۷۹ | تحلیل ترافیک شبکه ۲ | IPS_NTA_EXT.1.2 |
| ۸۰ | تحلیل ترافیک شبکه ۳ | IPS_NTA_EXT.1.3 |
| ۸۱ | کارکرد IPS مبتنی بر امضاء ۱ | IPS_SBD_EXT.1.1 |
| ۸۲ | کارکرد IPS مبتنی بر امضاء ۲ | IPS_SBD_EXT.1.2 |
| ۸۳ | کارکرد IPS مبتنی بر امضاء ۳ | IPS_SBD_EXT.1.3 |
| ۸۴ | کارکرد IPS مبتنی بر امضاء ۴ | IPS_SBD_EXT.1.4 |
| ۸۵ | کارکرد IPS مبتنی بر امضاء ۵ | IPS_SBD_EXT.1.5 |
| **الزامات مربوط به پیوست یک** | | |
| ۸۶ | ذخیره‌سازی رویدادهای ممیزی ۱ | FAU_STG.1.1 |
| ۸۷ | ذخیره‌سازی رویدادهای ممیزی ۲ | FAU_STG.1.2 |
| ۸۸ | محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی | FAU_STG_EXT.2.1/LocSpace |
| ۸۹ | ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی | FAU_STG.3.1/LocSpace |
| ۹۰ | محل ذخیره‌سازی داده‌های ممیزی IPS ۱ | FAU_STG_EXT.1.1 |
| ۹۱ | محل ذخیره‌سازی داده‌های ممیزی IPS ۲ | FAU_STG_EXT.1.2 |
| ۹۲ | محل ذخیره‌سازی داده‌های ممیزی IPS ۷ | FAU_STG_EXT.4.1 |
| ۹۳ | الزامات پروتکل X509(۱)/ تبادل داده کاربردی داخل محصول | FIA_X509_EXT.1.1/ITT |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۹۴ | الزامات پروتکل X509 (۲)/ تبادل داده کاربردی داخل محصول | FIA_X509_EXT.1.2/ITT |
| ۹۵ | مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها | FMT_MOF.1.1(1)/Services |
| ۹۶ | مدیریت داده‌های محصول ۱/ کلیدهای رمزنگاری | FMT_MTD.1.1/CryptoKeys |
| ۹۷ | مدیریت رفتار توابع امنیتی IPS ۱ | FMT_MOF.1.1 |
| ۹۸ | مدیریت داده‌های محصول IPS ۱ | FMT_MTD.1.1 |
| ۹۹ | انتقال داده امنیتی در داخل محصول ۱ | FPT_ITT.1.1 |
| ۱۰۰ | مسیر امن ۱/ پیوند زدن | FPT_TRP.1.1/Join |
| ۱۰۱ | مسیر امن ۲ / پیوند زدن | FPT_TRP.1.2/Join |
| ۱۰۲ | مسیر امن ۳ / پیوند زدن | FPT_TRP.1.3/Join |
| ۱۰۳ | تعریف کانال ثبت‌نام مؤلفه ۱ | FCO_CPC_EXT.1.1 |
| ۱۰۴ | تعریف کانال ثبت‌نام مؤلفه ۲ | FCO_CPC_EXT.1.2 |
| ۱۰۵ | تعریف کانال ثبت‌نام مؤلفه ۳ | FCO_CPC_EXT.1.3 |
| ۱۰۶ | حفظ وضعیت امن در زمان شکست ۱ | FPT_FLS.1.1 |
| ۱۰۷ | تخصیص منابع ۱ | FRU_RSA.1.1 |
| ۱۰۸ | فیلترینگ حالتمند پروتکل‌های پویا | FFW_RUL_EXT.2.1 |
| ۱۰۹ | نرمال‌سازی ترافیک ۱ | IPS_SBD_EXT.2.1 |
| ۱۱۰ | نرمال‌سازی ترافیک ۲ | IPS_SBD_EXT.2.2 |
| ۱۱۱ | نرمال‌سازی ترافیک ۳ | IPS_SBD_EXT.2.3 |
| **الزامات مربوط به پیوست دو** | | |
| ۱۱۲ | الزامات پروتکل DTLS Client (۱) | FCS_DTLSC_EXT.1.1 |
| ۱۱۳ | الزامات پروتکل DTLS Client (۲) | FCS_DTLSC_EXT.1.2 |
| ۱۱۴ | الزامات پروتکل DTLS Client (۳) | FCS_DTLSC_EXT.1.3 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۱۱۵ | الزامات پروتکل DTLS Client (۴) | FCS_DTLSC_EXT.1.4 |
| ۱۱۶ | الزامات پروتکل DTLS Client/ احراز هویت ۱ | FCS_DTLSC_EXT.2.1 |
| ۱۱۷ | الزامات پروتکل DTLS Client/ احراز هویت ۲ | FCS_DTLSC_EXT.2.2 |
| ۱۱۸ | الزامات پروتکل DTLS Client/ احراز هویت ۳ | FCS_DTLSC_EXT.2.3 |
| ۱۱۹ | الزامات پروتکل DTLS Client/ احراز هویت ۴ | FCS_DTLSC_EXT.2.4 |
| ۱۲۰ | الزامات پروتکل DTLS Client/ احراز هویت ۵ | FCS_DTLSC_EXT.2.5 |
| ۱۲۱ | الزامات پروتکل DTLS Client/ احراز هویت ۶ | FCS_DTLSC_EXT.2.6 |
| ۱۲۲ | الزامات پروتکل DTLS Client/ احراز هویت ۷ | FCS_DTLSC_EXT.2.7 |
| ۱۲۳ | الزامات پروتکل DTLS Server (۱) | FCS_DTLSS_EXT.1.1 |
| ۱۲۴ | الزامات پروتکل DTLS Server (۲) | FCS_DTLSS_EXT.1.2 |
| ۱۲۵ | الزامات پروتکل DTLS Server (۳) | FCS_DTLSS_EXT.1.3 |
| ۱۲۶ | الزامات پروتکل DTLS Server (۴) | FCS_DTLSS_EXT.1.4 |
| ۱۲۷ | الزامات پروتکل DTLS Server (۵) | FCS_DTLSS_EXT.1.5 |
| ۱۲۸ | الزامات پروتکل DTLS Server (۶) | FCS_DTLSS_EXT.1.6 |
| ۱۲۹ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱ | FCS_DTLSS_EXT.2.1 |
| ۱۳۰ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۲ | FCS_DTLSS_EXT.2.2 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۱۳۱ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۳ | FCS_DTLSS_EXT.2.3 |
| ۱۳۲ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۴ | FCS_DTLSS_EXT.2.4 |
| ۱۳۳ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۵ | FCS_DTLSS_EXT.2.5 |
| ۱۳۴ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۶ | FCS_DTLSS_EXT.2.6 |
| ۱۳۵ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۷ | FCS_DTLSS_EXT.2.7 |
| ۱۳۶ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۸ | FCS_DTLSS_EXT.2.8 |
| ۱۳۷ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۹ | FCS_DTLSS_EXT.2.9 |
| ۱۳۸ | الزامات پروتکل HTTPS (۱) | FCS HTTPS_EXT.1.1 |
| ۱۳۹ | الزامات پروتکل HTTPS (۲) | FCS_HTTPS_EXT.1.2 |
| ۱۴۰ | الزامات پروتکل HTTPS (۳) | FCS_HTTPS_EXT.1.3 |
| ۱۴۱ | الزامات پروتکل SSH Client (۱) | FCS_SSHC_EXT.1.1 |
| ۱۴۲ | الزامات پروتکل SSH Client (۲) | FCS_SSHC_EXT.1.2 |
| ۱۴۳ | الزامات پروتکل SSH Client (۳) | FCS_SSHC_EXT.1.3 |
| ۱۴۴ | الزامات پروتکل SSH Client (۴) | FCS_SSHC_EXT.1.4 |
| ۱۴۵ | الزامات پروتکل SSH Client (۵) | FCS_SSHC_EXT.1.5 |
| ۱۴۶ | الزامات پروتکل SSH Client (۶) | FCS_SSHC_EXT.1.6 |
| ۱۴۷ | الزامات پروتکل SSH Client (۷) | FCS_SSHC_EXT.1.7 |
| ۱۴۸ | الزامات پروتکل SSH Client (۸) | FCS_SSHC_EXT.1.8 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۱۴۹ | الزامات پروتکل SSH Client (۹) | FCS_SSHC_EXT.1.9 |
| ۱۵۰ | الزامات پروتکلSSH Server (۱) | FCS_SSHS_EXT.1.1 |
| ۱۵۱ | الزامات پروتکلSSH Server (۲) | FCS_SSHS_EXT.1.2 |
| ۱۵۲ | الزامات پروتکلSSH Server (۳) | FCS_SSHS_EXT.1.3 |
| ۱۵۳ | الزامات پروتکلSSH Server (۴) | FCS_SSHS_EXT.1.4 |
| ۱۵۴ | الزامات پروتکلSSH Server (۵) | FCS_SSHS_EXT.1.5 |
| ۱۵۵ | الزامات پروتکلSSH Server (۶) | FCS_SSHS_EXT.1.6 |
| ۱۵۶ | الزامات پروتکلSSH Server (۷) | FCS_SSHS_EXT.1.7 |
| ۱۵۷ | الزامات پروتکلSSH Server (۸) | FCS_SSHS_EXT.1.8 |
| ۱۵۸ | الزامات پروتکل TLS Client (۱) | FCS_TLSC_EXT.1.1 |
| ۱۵۹ | الزامات پروتکل TLS Client (۲) | FCS_TLSC_EXT.1.2 |
| ۱۶۰ | الزامات پروتکل TLS Client (۳) | FCS_TLSC_EXT.1.3 |
| ۱۶۱ | الزامات پروتکل TLS Client (۴) | FCS_TLSC_EXT.1.4 |
| ۱۶۲ | الزامات پروتکل TLS Client/ احراز هویت ۱ | FCS_TLSC_EXT.2.1 |
| ۱۶۳ | الزامات پروتکل TLS Client/ احراز هویت ۲ | FCS_TLSC_EXT.2.2 |
| ۱۶۴ | الزامات پروتکل TLS Client/ احراز هویت ۳ | FCS_TLSC_EXT.2.3 |
| ۱۶۵ | الزامات پروتکل TLS Client/ احراز هویت ۴ | FCS_TLSC_EXT.2.4 |
| ۱۶۶ | الزامات پروتکل TLS Client/ احراز هویت ۵ | FCS_TLSC_EXT.2.5 |
| ۱۶۷ | الزامات پروتکل TLS Server (۱) | FCS_TLSS_EXT.1.1 |
| ۱۶۸ | الزامات پروتکل TLS Server (۲) | FCS_TLSS_EXT.1.2 |
| ۱۶۹ | الزامات پروتکل TLS Server (۳) | FCS_TLSS_EXT.1.3 |
| ۱۷۰ | الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱ | FCS_TLSS_EXT.2.1 |
| ۱۷۱ | الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۲ | FCS_TLSS_EXT.2.2 |

| شماره الزام | نام الزام | عنصر متناظر با الزام |
|---|---|---|
| ۱۷۲ | الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳ | FCS_TLSS_EXT.2.3 |
| ۱۷۳ | الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۴ | FCS_TLSS_EXT.2.4 |
| ۱۷۴ | الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۵ | FCS_TLSS_EXT.2.5 |
| ۱۷۵ | الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۶ | FCS_TLSS_EXT.2.6 |
| ۱۷۶ | الزامات پروتکل X509(۱)/ ابطال | FIA_X509_EXT.1.1/Rev |
| ۱۷۷ | الزامات پروتکل X509(۱)/ ابطال | FIA_X509_EXT.1.2/Rev |
| ۱۷۸ | الزامات پروتکل X509(۳) | FIA_X509_EXT.2.1 |
| ۱۷۹ | الزامات پروتکل X509(۴) | FIA_X509_EXT.2.2 |
| ۱۸۰ | الزامات پروتکل X509(۵) | FIA_X509_EXT.3.1 |
| ۱۸۱ | الزامات پروتکل X509(۶) | FIA_X509_EXT.3.2 |
| ۱۸۲ | خودآزمایی محصول مورد ارزیابی ۲ | FPT_TST_EXT.2.1 |
| ۱۸۳ | الزامات به‌روزرسانی امن ۴ | FPT_TUD_EXT.2.1 |
| ۱۸۴ | الزامات به‌روزرسانی امن ۵ | FPT_TUD_EXT.2.2 |
| ۱۸۵ | مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار | FMT_MOF.1.1/AutoUpdate |
| ۱۸۶ | مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع | FMT_MOF.1.1/Functions |

## ۴,۱ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات عمدی و غیرعمدی موجود در زمینه پیکربندی و/یا کارکرد سیستم را در اختیاردارند، محصول باید این قابلیت را داشته باشد که

داده‌های ممیزی موردنیاز برای تشخیص چنین فعالیت‌هایی را تولید کند. ممیزی فعالیت‌های مدیریت سیستم سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سیستم، می‌توان برای طراحی اقدامات اصلاحی از آن‌ها استفاده کرد. ممیزی رویدادهای گزینش‌شده نشان می‌دهد که آیا بخش‌هایی مهم محصول مورد ارزیابی در معرض شکست قرار دارند یا خیر (مثلاً این‌که فرایند رمزنگاری اجرا نشود) و همچنین به شناسایی فعالیت‌های غیرمعمول (مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم) یک مورد مشکوک، کمک می‌کند. در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به‌اندازه‌ای زیاد شود که محصول مورد ارزیابی یا سرپرستان مسئول بازبینی این اطلاعات را دچار سردرگمی‌کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت مورد اعتماد خارجی ارسال کند. این اطلاعات باید دارای مهرهای زمانی قابل‌اعتماد باشند، این امر سبب می‌شود که بتوان اطلاعات را پس از ارسال به دستگاه‌های خارجی مرتب کرد. از دست رفتن ارتباط با سرور ممیزی می‌تواند مشکل‌ساز شود. 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:<br>الف) آغاز و اتمام توابع ممیزی؛<br>ب) تمامی رویدادهای قابل ممیزی برای سطوح ممیزی.<br>پ) تمام اقدامات مدیریتی شامل موارد زیر:<br>• ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود) | |

- تغییرات در داده‌های توابع امنیتی هدف ارزیابی مرتبط با تغییرات پیکربندی (علاوه بر اطلاعات حاکی از ایجاد تغییرات، باید تعیین شود که چه مواردی تغییر کرده‌اند)
- تولید/واردکردن، تغییر، یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز باید ثبت شود)
- تغییر گذرواژه (نام حساب کاربری مربوطه نیز باید ثبت شود)
- شروع و پایان توابع IPS
- همه رویدادهای متفاوت IPS
- همه واکنش‌های توابع IPS
- [انتخاب: [آغاز و توقف سرویس‌ها، هیچ اقدام دیگر، اختصاص:[لیست سایر کاربردهای ویژه]]]

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

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

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

**نکته کاربردی:**

در صورتی که لیست «اقدامات مدیریتی» ارائه شده در این الزام کارکردهای امنیتی محصول را به طور کامل پوشش ندهد، نویسنده سند هدف امنیتی باید با استفاده از قسمت «اختصاص» که در «انتخاب» قرارگرفته است اقدامات مدیریتی دیگری را به لیست اضافه کند.

برای اهداف ارزیابی توزیع‌شده، هر مؤلفه باید یک رکورد ممیزی برای الزامات کارکرد امنیتی که پیاده می‌کند، بیان کند. اگر زمانی که یک رویداد ممیزی برقرار می‌گردد، بیش از یک مؤلفه‌ی هدف ارزیابی درگیر باشد، آنگاه باید این رویداد برای تمامی مؤلفه‌های درگیر، ممیزی گردد (برای مثال، رد شدن یک ارتباط وقتی که یک مؤلفه قصد برقراری یک کانال ارتباط امن با مؤلفه‌ی دیگری را دارد، باید رویداد ممیزی آن توسط هر دو مؤلفه ثبت گردد). همچنین این فعالیت فقط محدود به پیغام‌های خطا نمی‌شود، بلکه عملیات موفق را نیز شامل می‌گردد.

**نکته کاربردی:**

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 کند:
الف) تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت[۱] فعال و نتیجه رویداد (موفقیت یا شکست)؛ و
ب) در مورد هر یک از انواع رویدادهای ممیزی و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در نکته کاربردی زیر مشخص‌شده است.

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

- برای الزام «مدیریت احراز هویت ناموفق» اطلاعات ممیزی تلاش‌های ناموفق که از تعداد مجاز بیشتر بوده است، ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.
- برای الزام «سازوکار احراز هویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای سازوکار تعیین هویت و احراز هویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد. برای الزام «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی، دستی ثبت می‌شود.
- برای الزام «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود.
- برای الزامات «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود.
- برای الزام «مهرهای زمانی[۲]» اطلاعات ممیزی مربوط به تغییرات صورت گرفته در زمان ثبت می‌شود. این اطلاعات باید شامل زمان‌های جدید و قدیم، منشأ تلاش (مانند آدرس IP) برای تغییر زمان موفق یا ناموفق باشد.
- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها ۷» اگر «قفل‌کردن» انتخاب شود، اطلاعات ممیزی تمام تلاش‌های صورت گرفته برای باز کردن قفل یک نشست تعاملی ثبت می‌شود. در صورتی که «خاتمه دادن» انتخاب شود، اطلاعات ممیزی مربوط به خاتمه دادن یک نشست محلی از طریق یک سازوکار قفل‌کردن نشست ثبت می‌شود
- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها ۵» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه دور از طریق یک سازوکار قفل‌کردن نشست ثبت می‌شود.

[۱] Subject
[۲] Time stamps

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

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

| نام الزام | رویدادهای ممیزی | اطلاعات اضافه رکوردهای ممیزی |
|---|---|---|
| مدیریت کارکرد محصول IPS ۱ | تغییرات در المان‌های خط‌مشی‌های IPS | شناسه‌ها یا نام المان‌های خط و مشی‌های IPS تغییر یافته (به عنوان نمونه کدام امضاء، مبنا، لیست‌های سیاه و سفید تغییر داده شده است) |
| کارکرد IPS مبتنی بر رفتار غیرعادی | ترافیک بازرسی شده که با خط‌مشی IPS مبتنی بر رفتار غیرعادی انطباق دارد. | آدرس‌های IP مبدأ و مقصد |
| | | محتوای فیلدهای سرآیند که با خط‌مشی‌های مشخص شده انطباق دارد. |
| | | واسطی که از آن بسته دریافت شده است. |
| | | جنبه‌های از خط‌مشی‌های قوانین مبتنی بر ناهنجاری که رویداد تریگر شده است (به عنوان نمونه گذردهی، زمان روز، فرکانس و ...). |

[۱] Drop

| | | |
|---|---|---|
| | | واکنش محصول در مقابل رویداد (اجازه داده شده است، مسدود شده است، هشدار مسدود شدن به فایروال ارسال شده است) |
| بلوکه کردن آدرس IP ۱ | انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا | آدرس‌های IP مبدأ و مقصد (و در صورت امکان، نشانه‌ای دال بر اینکه این آدرس‌های مبدأ و/یا مقصد منطبق با لیست هستند یا خیر) |
| | | واسط محصول که بسته را دریافت کرده است. |
| | | اقدامی که محصول در شبکه انجام می‌دهد (مانند اجازه دادن، مسدود کردن، ارسال دستور reset) |
| تحلیل ترافیک شبکه ۱ | تغییر اینکه کدام خط‌مشی‌های پیشگیری از نفوذ روی واسط محصول فعال هستند.<br><br>فعال کردن و غیرفعال کردن واسط محصول که خط‌مشی‌های پیشگیری از نفوذ روی آن اعمال شده‌اند.<br><br>تغییر اینکه کدام مُدها روی واسط محصول فعال هستند. | شناسایی واسط محصول |
| | | خط‌مشی پیشگیری از نفوذ و مد واسط (در صورت امکان) |
| کارکرد IPS مبتنی بر امضاء ۱ | انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا | نام یا شناسه امضای انطباق‌داده‌شده |
| | | آدرس‌های IP مبدأ و مقصد. |
| | | محتوای فیلدهای سرآیند که باید با خط‌مشی انطباق داشته باشند. |
| | | محصول که بسته را دریافت کرده است. |
| | | اقدامی که محصول در شبکه انجام می‌دهد (مانند اجازه دادن، مسدود کردن، ارسال دستور reset) |
| نرمال‌سازی ترافیک ۱ (اختیاری) | بازرسی بسته‌های کپسوله‌شده | شناسایی روش کپسوله‌سازی |

| | | |
|---|---|---|
| نرمال‌سازی ترافیک ۲ (اختیاری) | شکست در سر هم کردن مجدد بسته‌های چندتکه‌ای[۱] | آدرس‌های IP مبدأ و مقصد واسط محصول که تکه‌ها[۲] را دریافت کرده است. |
| نرمال‌سازی ترافیک ۳(اختیاری) | نرمال‌سازی ترافیک توسط محصول | آدرس‌های IP مبدأ و مقصد بسته‌های کنار گذاشته‌شده[۳] واسط محصول که بسته‌ها را دریافت کرده است |

**نکته کاربردی:**

رویدادهای ممیزی 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 کند.

| ۳ | **تولید داده ممیزی ۳** |
|---|---|

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

**نکته کاربردی:**

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

| ۴ | **محل ذخیره‌سازی داده‌های ممیزی ۱** |
|---|---|

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

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

**نکته کاربردی:**

محصول مورد ارزیابی برای انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به‌جز سرور محصول مورد ارزیابی استفاده می‌کند. ذخیره‌سازی این سوابق ممیزی و اجازه دادن به سرپرست

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

محصول جهت بازبینی این سوابق، توسط محیط عملیاتی صورت می‌گیرد. از آنجایی که سرور ممیزی خارجی قسمتی از محصول مورد ارزیابی نیست، به جزء توانایی‌های انتقال داده‌های ممیزی، الزاماتی برای آن تعریف نمی‌شود. همچنین برای قالب و پروتکل زیرساختی داده‌های ممیزی که باید انتقال یابند، الزاماتی تعیین نمی‌شود. محصول باید توانایی پیکربندی انتقال داده ممیزی به سرور خارجی را بدون مداخله سرپرست داشته باشد. انتقال دستی، نمی‌تواند الزامات را برآورده کند. ارسال باید به صورت بلادرنگ یا دوره‌ای انجام گیرد. اگر ارسال به صورت بلادرنگ انجام نشود، خلاصه مشخصات محصول چگونگی صورت گرفتن ارسال و بازه‌ی تکرار که محصول برای ارسال پشتیبانی می‌کند را توصیف می‌کند. خلاصه مشخصات محصول همچنین بازه‌ی تکرار قابل‌قبول را پیشنهاد می‌کند.

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

| ۵ | **محل ذخیره‌سازی داده‌های ممیزی ۲** |
|---|---|

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

| ۶ | **محل ذخیره‌سازی داده‌های ممیزی ۳** |
|---|---|

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

**نکته کاربردی:**

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

برای هر محصولات توزیع‌شده، نیاز نیست که هر مؤلفه داده‌های ممیزی را به صورت محلی ذخیره کند ولی به طور کلی محصول باید توانایی ذخیره‌ی محلی داده‌های ممیزی را داشته باشد. هر مؤلفه حداقل باید توانایی ذخیره موقت اطلاعات ممیزی برای مواردی که ارتباط شبکه دچار مشکل می‌شود را داشته باشد. ذخیره موقت نیاز نیست که بر روی حافظه ثابت صورت گیرد، این ذخیره محلی می‌تواند روی حافظه فرار انجام گیرد. برای هر مؤلفه که اطاعات را به صورت محلی ذخیره می‌کند یا اطلاعات ممیزی را به صورت موقت ذخیره می‌کند، باید مشخص شود هنگام پر شدن حافظه، چه اقدامی صورت گیرد.

[۱] Overwrite

[۲] External log server

## ۴,۲ پشتیبانی رمزنگاری (FCS)

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

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

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

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

**نکته کاربردی:**

نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورداستفاده برای استقرار کلید و 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 انتخاب باشند. درصورتی‌که برای احراز هویت دستگاه از الگوهای تولید کلید، غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و ecdsa-sha2-nistp521 استفاده شود، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی‌نامه X.509v3 باشد.

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

[۱] Key establishment

[۲] Keyed hash generation

| شماره الزام | نام الزام |
|---|---|
| در محصول مورد ارزیابی توزیع‌شده، اگر مؤلفه محصول به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند، محصول نیاز به پیاده‌سازی تولید کلید ندارد. | |
| ۸ | **مدیریت کلید رمزنگاری ۲** |

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

- الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56B بازبینی ۱، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛
- الگوهای استقرار کلید منحنی بیضوی[۳] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۴]؛
- الگوهای استقرار کلید میدانی[۵] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته».
- الگوی استقرار کلید با استفاده از دیفی-هلمن گروه ۱۴ که این الزامات را رعایت کنند: RFC 3526، بخش ۳؛

**نکته کاربردی:**

این عنصر درواقع نسخه اصلاح‌شده الزام «مدیریت کلید رمزنگاری ۲»[۶] در استاندارد ISO 15408 است که به‌جای توزیع کلید، به استقرار کلید می‌پردازد.

نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورداستفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. برای دیفی-هلمن گروه ۱۴، نویسنده هدف امنیتی باید به جای انتخاب استقرار کلید میدانی، از الزام کارکردی امنیتی یک انتخاب مناسب انجام دهد.

الگوهای استقرار کلید مبتنی بر RSA در بخش ۹، بازبینی ۱، مربوط به NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های بازبینی ۱ مربوط به SP 800-56B است.

توجه: اگر محصول مورد ارزیابی در الگوی استقرار کلید به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، الگوی تولید کلید RSA را اجرا کند.

---

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

| شماره الزام | نام الزام |
|---|---|
| منحنی‌های بیضوی مورداستفاده در الگوهای استقرار کلید، با منحنی‌های مشخص‌شده در الزام «مدیریت کلید رمزنگاری ۱» ارتباط دارند.<br>پارامترهای دامنه مورداستفاده در الگوهای استقرار کلید میدانی، به الگوهای تولید کلید مورداشاره در «مدیریت کلید رمزنگاری ۱» وابسته هستند. | |
| ۹ | **مدیریت کلید رمزنگاری ۴** |
| محصول مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: [اختصاص:<br>• برای کلیدهای متن-آشکار در ذخیره‌ساز فرار[۱]، نابودی باید از طریق یک [انتخاب: بازنویسی ساده شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]]، نابودی مرجع کلید که مستقیماً با درخواست زباله‌روبی همراه باشد] انجام شود.<br>• برای کلیدهای متن-آشکار در ذخیره‌ساز غیرفرار، نابودی باید از طریق فراخوان[۲] یک واسط مهیا شده توسط محصول مورد ارزیابی که [انتخاب:<br>○ به‌صورت منطقی مکان ذخیره‌سازی کلید را آدرس می‌دهد و یک بازنویسی [انتخاب: ساده، [اختصاص: تعداد عبورها]-عبور] شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]] را انجام می‌دهد.<br>○ یک بخشی از توابع امنیتی محصول را برای نابودی انتزاع معرف کلید، می‌سازد]<br>انجام شود.]<br>**نکته کاربردی:**<br>در قسمت مربوط به انتخاب در گزینه دوم از اولین اختصاص، جایی که کلیدها برای نابودی به‌وسیله «یک بخشی از توابع امنیتی محصول» شناسایی می‌شوند، خلاصه مشخصات محصول باید «بخش» مربوطه و واسط مرتبط با آن را تعریف کند. واسط اشاره شده در الزام می‌تواند در محصولات مختلف، شکل متفاوتی داشته باشد. شاید مشهودترین شکل آن یک برنامه کاربردی روی یک سیستم‌عامل باشد.<br>وقتی که روش‌های تخریب مختلفی برای کلیدهای مختلف و/یا موقعیت‌های تخریب مختلف استفاده می‌شود، این روش‌ها و کلیدها/موقعیت‌های متفاوت بکار گرفته شده، در خلاصه مشخصات محصول توصیف می‌شوند. خلاصه مشخصات محصول همه | |

[۱] Volatile Storage

[۲] Invocation

| شماره الزام | نام الزام |
|---|---|
| کلیدهای مرتبط استفاده شده در پیاده‌سازی الزامات کارکرد امنیتی را توصیف می‌کند، همچنین مواردی که محل ذخیره شدن کلیدها به‌صورت متن آشکار است را شامل می‌شود.<br>در بعضی از اختصاص‌های بالا، از «شامل هیچ CSP نباشد» استفاده شده است. این جمله به این معنی است که محصول از برخی داده خاص استفاده می‌کند که شامل هیچ‌کدام از مقادیر تولید شده توسط تولیدکننده بیت تصادفی موجود در الزام FCS_RBG_EXT یا مقادیر مشخص لیست شده در این الزام، مثلاً موارد لیست شده در اولین انتخاب از اولین اختصاص این الزام نیست. در واقع وجود عبارت «شامل هیچ CSP نباشد» برای مطمئن شدن از این موضوع است که حتماً بازنویسی داده با دقت انتخاب شده است.<br>لازم به ذکر است که کلیدهای رمزنگاری در این الزام، شامل کلیدهای نشست نیز می‌شود. همچنین تخریب کلید برای مؤلفه عمومی در جفت کلید نامتقارن، اعمال نمی‌شود. | |
| ۱۰ | **عملیات رمزنگاری ۱ (۱)** |
| محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص [اختصاص: الگوریتم AES که در حالت [انتخاب: CBC، GCM، CTR] و در اندازه‌های کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] استفاده می‌شوند] و با توجه به [اختصاص: استاندارد AES که در ISO 18033-3 تعریف‌شده است، [انتخاب: CBC که در ISO 10116 تعریف‌شده است، GCM که در ISO 19772 تعریف‌شده است، CTR که در ISO 10116 تعریف شده است]] انجام دهد.<br>**نکته کاربردی:**<br>در مورد نخستین انتخاب این الزام، نویسنده هدف امنیتی حالت یا حالت‌های کارکردی AES را انتخاب می‌کند. در مورد دومین انتخاب، نویسنده هدف امنیتی اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب می‌کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[۱] در الزامات کانال امن هستند. | |
| ۱۱ | **عملیات رمزنگاری ۱ (۲)** |
| محصول مورد ارزیابی باید سرویس‌ها امضای رمزنگاری (تولید و تائید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب:<br>• الگوریتم امضای دیجیتال RSA و کلید رمزنگاری با اندازه‌های (ماژول‌ها) [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر]<br>• الگوریتم امضای دیجیتال بیضوی و کلید رمزنگاری با اندازه‌های [اختصاص: ۲۵۶ بیتی یا بزرگ‌تر]<br>]<br>با رعایت موارد زیر: | |

[۱] Cipher suite

| شماره الزام | نام الزام |
|---|---|
| [انتخاب:<br>• در مورد الگوهای RSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵,۵، با استفاده از الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳،<br>• در مورد الگوهای ECDSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، با اجرای منحنی‌های [انتخاب: P-256، P-384، P-521]؛ ISO/IEC 14888-3، بخش ۶,۴<br>]<br>**نکته کاربردی:**<br>نویسنده هدف امنیتی الگوریتم(های) مورد استفاده برای اجرای امضای دیجیتال را انتخاب می‌کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی انتخاب‌ها و اختصاص‌های مناسب را انجام می‌دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین می کند. نویسنده هدف امنیتی، با استفاده از انتخاب‌ها و اختصاص‌های این الزام، از شامل شدن تمامی مقادیر پارامترهای ضروری برای مجموعه رمز انتخاب شده به‌وسیله الزامات سند هدف امنیتی، اطمینان پیدا می‌کند. نویسنده هدف امنیتی همچنین سازگار بودن انتخاب‌های انجام گرفته شده با دیگر الزامات رمزنگاری را بررسی می‌کند، خصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی شود. | |
| ۱۲ | **عملیات رمزنگاری ۱ (۳)** |
| محصول مورد ارزیابی باید سرویس‌ها درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1، SHA-256، SHA-384، SHA-512 ] و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی که [اختصاص: ISO/IEC 10118-3:2004] را رعایت کند، ارائه کند.<br><br>**نکته کاربردی:**<br>به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌کنند، 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.<br>توجه: طبق SP 800-131 A الگوریتم SHA-1 فقط می‌تواند برای عملیات غیر از امضای دیجیتال همچون درهم سازی رمز عبور و ... استفاده شود. در نسخه‌های آتی این پروفایل حفاظتی، SHA-256 کمینه الزام برای محصولات خواهد بود. | |

| شماره الزام | نام الزام |
|---|---|
| انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای الزام «عملیات رمزنگاری ۱(۱)» و الزام «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی). | |
| ۱۳ | **عملیات رمزنگاری ۱ (۴)** |
| محصول مورد ارزیابی باید 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 اندازه‌های کلید [اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)] و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح‌شده در [اختصاص: بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم MAC ۲»] انجام دهد.<br>**نکته کاربردی:**<br>اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که L2<=k<=L1. | |
| ۱۴ | **تولید بیت تصادفی ۱** |
| محصول مورد ارزیابی باید سرویس‌ها تولید بیت تصادفی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG، HMAC_DRBG، CTR_DRBG (AES)] ارائه دهد. | |
| ۱۵ | **تولید بیت تصادفی ۲** |
| RBG قطعی باید دست‌کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم‌افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت‌افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست‌کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و CSPs که تولید می‌کند، مطابق با ISO/IEC 18031:2011، باشد.<br><br>**نکته کاربردی:**<br>در مورد نخستین عبارت این الزام، نویسنده هدف امنیتی حداقل یکی از انواع منابع نویز را انتخاب می‌کند. اگر محصول مورد ارزیابی شامل چند منبع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی از هر یک از انواع منابع پر می‌کند (مثلاً دو منبع نویز مبتنی بر نرم‌افزار و یک منبع نویز مبتنی بر سخت‌افزار). مستندات و آزمون‌های مورد نیاز در فعالیت‌های ارزیابی، باید تکرار گردند تا تمام منابع مشخص شده در هدف امنیتی را پوشش دهند. سند ISO/IEC 18031:2011 | |

[1] Keyed-hash message authentication

| شماره الزام | نام الزام |
|---|---|
| شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها به عناصر اولیه فرایند رمزنگاری (توابع درهم‌ساز و مجموعه‌های رمز) بستگی دارد. نویسنده هدف امنیتی، تابع استفاده شده و شامل عناصر اولیه فرایند رمزنگاری را که در الزام بکار گرفته شده است، انتخاب خواهد کرد. با اینکه تمام توابع درهم‌ساز تعیین‌شده (SHA-1، SHA-256، SHA-384، SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، در پیاده‌سازی‌های CTR_DRBG تنها موارد مبتنی بر AES اجازه استفاده دارند.<br>اگر اندازه کلید برای پیاده‌سازی AES متفاوت با اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تغییر یا تکرار «عملیات رمزنگاری» باشد تا تفاوت اندازه کلید در آن لحاظ گردد. در قسمت انتخاب تعداد بیت آنتروپی مربوط به این الزام، نویسنده هدف امنیتی حداقل تعداد بیت‌های انتروپی تزریق‌شده به RBG را انتخاب می‌کند که این مقدار باید بزرگ‌تر یا مساوی طول هر کلید امنیتی باشد که توسط محصول تولید می‌شود. | |

### ۴,۳ 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 غیرقابل‌اعتماد دیگر بگذرد. کارکرد امنیتی محصول UTM باید این قابلیت را داشته باشد که از ترافیک حساس منتقل‌شده حفاظت کند (مانند ترافیک سرپرست محصول، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست). یکی از راه‌های ایجاد کانال ارتباطی بین محصول UTM و یک موجودیت IT خارجی، به گونه‌ای که این ارتباط را بتوان از هر دو طرف احراز هویت کرد، استفاده از IPsec است. IPsec یک پروتکل همتا به همتا است و بنابراین نیازی به تفکیک الزامات کلاینت و سرور وجود ندارد.

| شماره الزام | نام الزام |
|---|---|
| ۱۶ | **الزامات پروتکل IPSEC (۱)** |
| محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آنچه در RFC 4301 مشخص شده است، پیاده‌سازی کند.<br><br>**نکته کاربردی:**<br>بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه‌داده خط‌مشی امنیتی (SPD) استفاده کرد. با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند:<br>۱- «PROTECT» از بسته‌ها (مثلاً رمزگذاری آن‌ها) | |

۲- «BYPASS» سرویس‌های IPSEC (مثلاً عدم رمزگذاری)

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

پایگاه‌داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به لیست‌های کنترل دسترسی به مسیریاب، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف‌نظر از روشی که به کار گرفته می‌شود، مفهومی به نام «قانون[۱]» وجود دارد که بسته‌ها با آن «مطابقت» می‌کنند و در نتیجه یک اقدام انجام می‌گیرد.

باید ابزارهایی برای مرتب کردن این قوانین وجود داشته باشد، ولی داشتن یک رویکرد عمومی در این زمینه الزام نشده است. قاعده کلی این است که SPD باید بتواند بسته‌های IP را از یکدیگر تمایز دهد و قوانین مربوطه را در مورد آن‌ها اعمال کند. ممکن است چند SPD وجود داشته باشند (یک پایگاه داده برای هر واسط شبکه)، اما الزامی در این زمینه وجود ندارد.

| ۱۷ | **الزامات پروتکل IPSEC (۲)** |
|---|---|

محصول مورد ارزیابی باید مقدار/قانون در پایگاه داده SPD، برای تمام موارد غیر منطبق داشته باشد و آن‌ها را طبق آن مقدار/قانون دور بریزد.

| ۱۸ | **الزامات پروتکل IPSEC (۳)** |
|---|---|

محصول مورد ارزیابی باید [انتخاب: مد انتقال، مد تونل] را پیاده‌سازی کند.

**نکته کاربردی:**

نویسنده سند هدف امنیتی باید مدهای عملیاتی پشتیبانی شده برای IPSec را مشخص کند.

| ۱۹ | **الزامات پروتکل IPSEC (۴)** |
|---|---|

محصول مورد ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است فریمورک ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-128، AES-CBC-128 (تشریح شده در RFC 3602)، هیچ الگوریتم دیگری] به همراه یک HMAC مبتنی بر الگوریتم درهم‌سازی امن (SHA) [انتخاب: HMAC-SHA-1، HMAC-SHA-256، HMAC-SHA-384، HMAC-SHA-512، هیچ الگوریتم دیگری] و [انتخاب: AES-GCM-128، AES-GCM-192، AES-GCM-256 (تشریح شده در RFC 4106)، هیچ الگوریتم دیگری] پیاده‌سازی کند.

**نکته کاربردی:**

وقتی که الگوریتم AES-CBC انتخاب گردد، حداقل یک HMAC مبتنی بر SHA نیز باید انتخاب شود. اگر یک AES-GCM انتخاب گردد، نیاز نیست که HMAC انتخاب شود زیرا AES-GCM محرمانگی و جامعیت را فراهم می‌کند. در صورتی که برای IPSec با توجه

[۱] rule

| |
|---|
| به خروجی مورد انتظار، نوع خاصی از HMAC مبتنی بر SHA (مثلاً، HMAC کوتاه شده[۱]) انتخاب گردد، در خلاصه مشخصات محصول باید مشخص شود. |
| **۲۰** \| **الزامات پروتکل IPSEC (۵)** |
| محصول مورد ارزیابی باید یکی از این پروتکل‌ها را به کار گیرد: [انتخاب:<br>• IKEv1، با استفاده از مد اصلی[۲] برای انتقال در فاز اول، طبق آنچه در RFC 4109, 2408, 2409, RFCs 2407، [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] بیان شده است.<br><br>• IKEv2، مطابق با آنچه در RFC 5996 و [انتخاب: بدون پشتیبانی از پیمایش NAT[۳]، با پشتیبانی اجباری از پیمایش NAT چنان‌که در بخش ۲,۲۳ از RFC 5996 تشریح شده است] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز] تشریح شده است.<br>].<br>**نکته کاربردی:**<br>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 کند. اگر محصول از HMACs مبتنی بر SHA، کوتاه‌شده مطابق با RFC 4868 استفاده کند، باید در خلاصه مشخصات محصول، مشخص گردد. |
| **۲۱** \| **الزامات پروتکل IPSEC (۶)** |
| محصول مورد ارزیابی باید اطمینان حاصل کند که برای پی‌آیند (پایه‌بار)[۴] رمزگذاری‌شده در پروتکل [انتخاب: IKEv2،IKEv1]، از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256 (تشریح شده در RFC 3602)، AES-GCM-128، AES-GCM-192، AES-GCM-256 (تشریح شده در RFC 5282) استفاده می‌شود.<br><br>**نکته کاربردی:**<br>از آنجایی که هیچ RFC وجود ندارد که AES-GCM را برای IKEv1 تعریف کرده باشد، AES-GCM-128، AES-GCM-192 و AES-GCM-256 تنها در صورتی انتخاب می‌شوند که IKEv2 نیز انتخاب شده باشد. |

[۱] Truncated
[۲] Main Mode
[۳] NAT traversal
[۴] Payload

| ۲۲ | الزامات پروتکل IPSEC (۷) |
|---|---|

محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب:

- سرپرست محصول می‌تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب:
  - تعداد بایت‌ها؛
  - مدت‌زمان 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:
  - تعداد بایت‌ها؛
  - مدت‌زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد؛ ] پیکربندی کند.

**نکته کاربردی:**

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در «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 مدت‌زمان 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 مدت‌زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

| ۲۳ | 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:
  - تعداد بایت‌ها؛
  - مدت‌زمان 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:
  - تعداد بایت‌ها؛
  - مدت‌زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد؛ ] پیکربندی کند.

**نکته کاربردی:**

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در «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 مدت‌زمان 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 مدت‌زمان‌های SA را باید در سند شرح محصول در نظر گرفت. |
| **۲۴ \| الزامات پروتکل IPSEC (۹)** |
| محصول باید مقدار x را که در تبادل کلید IKE DiffieHellman (x در $g^x \bmod p$) به کار می‌رود، با استفاده از تولیدکننده بیت تصادفی که در الزام «تولید بیت تصادفی ۱» مشخص شده است و دست‌کم طول آن [اختصاص: تعداد بیت‌های (یک یا بیش از یک) باشد که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره شده باشد] تولید کند.<br><br>**نکته کاربردی:**<br>در گروه‌های ۱۹ و ۲۰ دیفی‌هلمن، مقدار "x" ضریب نقطه‌ای برای g است.<br>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. نویسند سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در مستند 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 مقدار منحصربه‌فرد برای پر کردن قسمت اختصاص 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. |
| **۲۵ \| الزامات پروتکل IPSEC (۱۰)** |
| محصول باید نانس‌های مورداستفاده در تبادلات [انتخاب: IKEv1، IKEv2] را با طول [انتخاب:<br>▪ [اختصاص: قدرت امنیتی مربوط به گروه Diffie-Hellman مذاکره شده]؛<br>▪ حداقل ۱۲۸ بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی[۱] مذاکره شده (PRF)] تولید کند.<br>**نکته کاربردی:**<br>اگر IKEv2 انتخاب شده باشد (همان‌طور که در RFC5996 اجباری شده است)، نویسنده سند هدف امنیتی باید دومین گزینه را برای طول نانس انتخاب کند. نویسنده سند هدف امنیتی مجاز است هر یک از گزینه‌ها را برای IKEv1 انتخاب کند. |

[۱] Pseudorandom Function hash

| |
|---|
| در اولین گزینه برای طول نانس، از آنجایی که در پیاده‌سازی ممکن است برای استفاده از گروه‌های مختلف Diffie-Hellman در ساخت تضمین‌های امنیتی، مذاکره کردن مجاز باشد، اختصاص مربوط به «الزامات پروتکل IPSEC (۱۰)» می‌تواند مقادیر متعددی داشته باشد.<br>نویسنده سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در مستند 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 مقدار منحصربه‌فرد برای پر کردن قسمت اختصاص 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 گروه DH مذاکره شود، مبادله شوند، بنابراین توصیه می‌شود نانس به‌کاررفته به اندازه کافی بزرگ باشد که همه پیشنهادهای محصول انتخاب‌شده در تبادل را پشتیبانی کند. |

| ۲۶ | **الزامات پروتکل IPSEC (۱۱)** |
|---|---|
| محصول باید اطمینان حاصل کند که پروتکل‌های IKE، همه گروه(های) DH [انتخاب: ۱۴ (2048-bit MODP) و ۱۹ (256-bit Random ECP)، ۲۰ (384-bit Random ECP)، ۲۴ (2048-bit MODP به همراه 256-bit POS)] را پشتیبانی می‌کنند. | |
| **نکته کاربردی:**<br>قسمت «انتخاب» در این الزام جهت مشخص کردن این موضوع که گروه‌های DH اضافه پشتیبانی شده است، بکار می‌رود. این الزام برای هر دو IKEv1 و IKEv2 اعمال می‌گردد. | |

| ۲۷ | **الزامات پروتکل IPSEC (۱۲)** |
|---|---|
| محصول باید به صورت پیش‌فرض بتواند اطمینان حاصل کند که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۱ IKEv1، IKEv2 IKE_SA] مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۲ IKEv1، IKEv2 CHILD_SA] مذاکره شده است، باشد. | |
| **نکته کاربردی:**<br>نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام‌یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند. انتخاب نسخه(های) IKE نه فقط در این الزام بلکه در تمامی الزامات بخش IPSec، باید سازگار باشد. | |

| ۲۸ | **الزامات پروتکل IPSEC (۱۳)** |
|---|---|
| محصول باید اطمینان حاصل کند که همه پروتکل‌های IKE احراز هویت همتا را با استفاده از [انتخاب: RSA، ECDSA] که از گواهی‌های X.509v3 مطابق با RFC4945 و [انتخاب: کلیدهای پیش‌اشتراکی، هیچ روش دیگری] استفاده می‌کند، انجام می‌دهند. | |

**نکته کاربردی:**

برای انطباق با این پروفایل حفاظتی، حداقل یک روش احراز هویت همتا مبتنی بر کلید عمومی لازم است؛ نویسنده سند هدف امنیتی باید اطمینان حاصل کند که الزامات کلاس رمزنگاری متناسب که نشان دهنده الگوریتم‌های استفاده شده (و سازگاری کلیدهای تولید شده) برای پشتیبانی روش انتخابی است، ارائه شده باشد. خلاصه مشخصات محصول باید تشریح کند که چگونه الگوریتم‌ها مورد استفاده قرار می‌گیرند (برای مثال؛ RFC 2409 سه روش احراز هویت با استفاده از کلید عمومی را مشخص می‌کند، هر کدام که استفاده می‌شود باید در خلاصه مشخصات محصول ذکر گردد).

| ۲۹ | **الزامات پروتکل IPSEC (۱۴)** |
|---|---|

محصول باید کانال امن را فقط در صورتی که شناساننده موجود در گواهی‌نامه دریافتی با شناساننده مرجع پیکربندی شده انطباق داشته باشد، برقرار کند. شناساننده مرجع و ارائه شده از انواع زیر می‌باشند:

[ انتخاب: آدرس IP، FQDN[۱]، FQDN کاربر، نام متمایز شده (DN[۲])] و[انتخاب: هیچ نوع شناساننده مرجع دیگری، [انتخاب: دیگر انواع شناساننده مرجع پشتیبانی شده]] .

**نکته کاربردی:**

وقتی که از گواهی‌نامه‌های RSA یا ECDSA برای احراز هویت همتا استفاده می‌گردد، شناساننده مرجع و ارائه شده یکی از فرم‌های FQDN، DN، آدرس IP یا FQDN کاربر را پیدا می‌کند. لازم به ذکر است که شناساننده مرجع، در واقع همان شناساننده‌ای است که محصول انتظار دارد از IKE احراز هویت کاربر دریافت کند. همچنین شناساننده ارائه شده، شناساننده‌ای است که در بدنه گواهی‌نامه ارائه می‌شود.

روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه[۳]، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود.

[۱] Fully Qualified Domain Name

[۲] Distinquished Name

[۳] Background

### ۴,۴ 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 دسترس خواهد بود.

| شماره الزام | نام الزام |
|---|---|
| ۳۰ | **فیلترینگ حالتمند ۱** |
| محصول، باید بر روی بسته‌های شبکه‌ای که توسط محصول پردازش می‌شود، فیلتر ترافیک را انجام دهد.<br>نکته کاربردی:<br>کلاس فایروال دارای یک عنصر به نام فیلتر کردن حالتمند ترافیک شبکه است که بر روی بسته‌های پردازش شده توسط محصول اعمال می‌گردد. فایروال‌هایی 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.<br>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. | |
| ۳۱ | **فیلترینگ حالتمند ۲** |
| محصول، باید قوانین فیلتر کردن ترافیک را با استفاده از فیلدهای پروتکل شبکه زیر و واسط‌های مجزا تعریف کند: | |

- 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:

این مؤلفه در زمان ایجاد قوانینی که توسط این الزام اجرا می‌گردند، ویژگی‌های مختلف قابل به‌کارگیری را تعریف می‌کند. همچنین «واسط» که در بالا معرفی شده است پورت خروجی است که ترافیک شبکه اجرایی را دریافت و یا به طور متناوب ارسال خواهد کرد.

| ۳۲ | **فیلترینگ حالتمند ۳** |
|---|---|

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

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

نکته کاربردی:

این عنصر، عملکردهایی را تعریف می‌کند 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.

| ۳۳ | **فیلترینگ حالتمند ۴** |
|---|---|

محصول، باید امکان اعمال هر یک از قوانین فیلتر کردن حالتمند شبکه را بر روی هر یک از واسط‌های شبکه فراهم آورد.

نکته کاربردی:

این عنصر محل اعمال قوانین را مشخص می‌کند. یک محصول مطابق با این پروفایل حفاظتی، باید قادر باشد که قوانین فیلتر کردن 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 کند. قابل شناسایی به این معنی است که واسط‌ها در داخل محصول منحصربه فرد و قابل شناسایی است و لزوماً به واسطی که از دید شبکه قابل مشاهده باشد، اشاره ندارد (به طور مثال لازم نیست که 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.

| ۳۴ | **فیلترینگ حالتمند ۵** |
|---|---|

محصول باید:

الف) بسته‌های شبکه را بدون پردازش قوانین مربوط به فیلتر کردن حالتمند ترافیک قبول کند، 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: **لیستی از ویژگی‌های تطبیق**]»، هیچ پروتکل دیگری]*

ب) جریان ترافیک موجود را از مجموعه جریان ترافیک ایجاد شده بر اساس [ انتخاب: *مدت‌زمان غیرفعال بودن نشست، اتمام جریان اطلاعات مورد انتظار*]، حذف کند.

نکته کاربردی:

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 کند. هم‌چنین این الزام صفات عملی را که برای تطابق و تعیین نشست شروع شده با بسته‌های شبکه مورد استفاده قرار می‌گیرند، مشخص می‌کند.

چنانچه ICMP به عنوان پروتکل انتخاب گردد، آدرس مبدأ و آدرس مقصد برای تعیین تعلق یک بسته به ارتباط شروع شده قبلی استفاده می‌شود. 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 کنند.

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 کنند، از بخش «اختصاص» کمک گرفته می‌شود.

در قسمت دوم از عنصر بالا، لازم است که مشخص گردد که فایروال چگونه می‌تواند جریان اطلاعات برقرار شده از مجموعه جریان اطلاعاتی برقرارشده بر اساس مشاهده یک رویداد حذف کند. 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 کند.

| **۳۵** | **فیلترینگ حالتمند ۶** |
|---|---|

محصول، باید قوانین فیلتر کردن حالتمند شبکه زیر را به طور پیش‌فرض بر روی تمام ترافیک شبکه اعمال کند:

[۱] Sequence number

۱- محصول باید بسته‌های اطلاعاتی را که به صورت نامعتبر قطعه‌بندی شده‌اند رد کند و قادر به [انتخاب: شمردن، ثبت] آن‌ها باشد.
۲- محصول باید بسته‌های IP قطعه‌بندی شده‌ای را که نمی‌توانند به طور کامل دوباره گردآوری شوند رد کند و قادر به [انتخاب: شمردن، ثبت] آن‌ها باشد.
۳- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد کند 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 کند 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 کند 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 کند 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.
۶- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه را رد کند 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 آینده» (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 کند 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*]

| ۳۶ | **فیلترینگ حالتمند ۷** |
|---|---|

محصول، باید قادر به حذف و ثبت مطابق با قوانین زیر باشد:
۱- محصول باید آن دسته از بسته‌های اطلاعاتی شبکه که آدرس مبدأ آن با آدرس واسط شبکه‌ای که بسته‌های اطلاعاتی شبکه را دریافت کرده برابر باشد را کنار بگذارد و قادر به ثبت باشد.

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

| | |
|---|---|
| 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.<br>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. | |
| **۳۷** | **فیلترینگ حالتمند ۸** |
| محصول باید قادر باشد قوانین اجرایی فیلتر کردن حالتمند ترافیک را به ترتیب تعیین شده توسط سرپرست محصول، پردازش کند. | |
| **۳۸** | **فیلترینگ حالتمند ۹** |
| محصول باید مانع از عبور جریان بسته‌های شود که هیچ قانونی برای آن مشخص نشده است. | |
| **۳۹** | **فیلترینگ حالتمند ۱۰** |
| محصول باید قادر باشد تعداد اتصالات نیمه‌باز TCP را مطابق با تعریف سرپرست سیستم محدود کند. برای رویدادهای که مقدار آن به مقدار حد پیکربندی می‌رسد، اتصالات جدید باید حذف و رویداد حذف شده باید [انتخاب: شمرده، ثبت] شود. | |

### ۴,۵ کلاس شناسایی و احراز هویت

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

| شماره الزام | نام الزام |
|---|---|
| **۴۰** | **مدیریت احراز هویت ناموفق ۱** |
| محصول مورد ارزیابی باید وقتی که یک عدد مثبت قابل تنظیم توسط سرپرست در [اختصاص: بازه مقادیر قابل‌قبول]، از تلاش‌های ناموفق احراز هویت مرتبط با تلاش‌های سرپرستان برای احراز هویت راه دور اتفاق میافتد را تشخیص دهد. | |

| ۴۱ | مدیریت احراز هویت ناموفق ۲ |
|---|---|

زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده برسد، محصول مورد ارزیابی باید [انتخاب: سرپرست راه دور تخطی‌کننده را از احراز هویت موفق جلوگیری کند تا وقتی که یک [اختصاص: اقدام] توسط یک سرپرست محلی صورت گیرد، سرپرست راه دور تخطی‌کننده را از احراز هویت موفق جلوگیری کند تا وقتی که یک دوره زمانی تعریف شده توسط سرپرست سپری شود.] انجام دهد.

**نکته کاربردی:**

این الزام روی یک تعداد تلاش پی‌درپی احراز هویت ناموفق اعمال می‌شود و برای یک سرپرست در کنسول محلی اعمال نمی‌گردد، زیرا قفل‌کردن یک سرپرست محلی، مدنظر نیست. نیل به این مهم نیازمند وجود حساب‌های سرپرستی محلی و راه دور جداگانه یا داشتن سازوکار احراز هویتی است که بتواند تلاش‌های ورود سرپرست محلی و راه دور را به‌صورت متمایز پیاده‌سازی کند. عبارت «اقدام» در اختصاص این الزام، توسط یک سرپرست محلی اتخاذ می‌گردد و در واقع یک پیاده‌سازی خاص است که توسط راهنمای سرپرست[۱] تعریف می‌شود (مثل بازنشاندن رمز عبور[۲]، بازنشاندن قفل[۳]). نویسنده هدف امنیتی یک از گزینه‌های انتخاب در این الزام را برای کنترل کردن شکست‌های احراز هویت، بسته به نوع پیاده‌سازی کنترل‌کننده در محصول، گزینش می‌کند.

خلاصه مشخصات محصول باید توصیف کند که محصول چگونه این اطمینان را ایجاد می‌کند که مسدود شدن موقت یا دائم یک سرپرست راه دور به دلیل شکست‌های احراز هویت، باعث به وجود آمدن عدم دسترس‌پذیری سرپرست نمی‌گردد (مثال: با تعریف کردن یک ورود محلی که مسدودسازی برای آن اعمال نمی‌شود). راهنمای محیط عملیاتی مشخص می‌سازد که چگونه همیشه یک دسترسی سرپرست نگه‌داری می‌شود حتی در صورتی که یک سرپرست راه دور در اثر موارد مطرح شده در این الزام، مسدود گردد.

| ۴۲ | مدیریت رمز عبور ۱ |
|---|---|

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

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

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

**نکته کاربردی:**

[۱] Administrator guidance

[۲] Password reset

[۳] Lockout reset

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

اختصاص مطرح شده در بند ب، باید به بزرگ‌ترین مقداری که می‌تواند برای کمینه طول رمز عبور توسط سرپرست پیکربندی شود، تنظیم گردد.

| ۴۳ | **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:

- نمایش بنر اخطار با توجه به الزام FTA_TAB.1
- [انتخاب: هیچ اقدامی، [اختصاص: لیست سرویس‌ها، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های خارجی]]

| ۴۴ | **شناسایی و احراز هویت کاربر ۲** |
|---|---|

پیش از آن که محصول مورد ارزیابی امکان انجام اقدامات مدیریتی سیستم را فراهم آورد، باید هر مدیر سیستم را ملزم کند که به صورت موفق شناسایی و احراز هویت گردد.

**نکته کاربردی:**

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

احراز هویت می‌تواند مبتنی بر گذرواژه باشد و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از گذرواژه‌ها پشتیبانی می‌کند (مانند SSH)، یا اینکه بر اساس گواهی‌نامه انجام شود (مانند SSH و TLS).

در مورد ارتباط با موجودیت‌های IT خارجی (مانند یک سرور ممیزی یا سرور NTP) این ارتباطات باید بر اساس الزام‌های FTP_ITC.1 انجام شوند که پروتکل آن از شناسایی و 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 شناسایی و احراز هویت است.

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

| ۴۵ | **سازوکار احراز هویت بر اساس رمز عبور ۲** |
|---|---|

محصول مورد ارزیابی باید یک سازوکار محلی احراز هویت مبتنی بر گذرواژه و [انتخاب: [اختصاص: سایر سازوکارهای احراز هویت]، هیچ سازوکار دیگری] را برای احراز هویت کاربر محلی مدیر سیستم فراهم آورد.

**نکته کاربردی:**

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

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

| ۴۶ | **احراز هویت کاربر ۱۰** |
|---|---|

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

**نکته کاربردی:**

«بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی داده‌های 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).

[۱] Obscured feedback

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.

### ۴,۶ کلاس مدیریت امنیت

توابع مدیریتی مورد نیاز در این بخش، شامل قابلیت‌های مورد نیاز برای پشتیبانی از نقش سرپرست امنیتی محصول و همچنین مجموعه‌ای از توابع مدیریتی امنیت مورد نیاز برای مدیریت بخش‌های قابل پیکربندی الزامات کارکرد امنیتی (FMT_SMF.1)، مدیریت کلی داده‌های توابع امنیتی محصول (FMT_MTD.1/CoreData) و فعال کردن به‌روزرسانی‌های محصول (FMT_MOF.1/ManualUpdate) هستند.

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

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

| شماره الزام | نام الزام |
|---|---|
| ۴۷ | **مدیریت کارکرد در محصول IPS۱** |
| محصول مورد ارزیابی باید قادر به انجام توابع مدیریتی زیر باشد:<br>]<br>۱) فعال‌سازی، غیر فعال‌سازی امضاهایی که در واسط‌های حسگر به کار می‌روند و تعیین رفتار کارکرد IPS<br>۲) تغییر و اصلاح این پارامترهایی که جمع‌آوری و تحلیل ترافیک شبکه را تعیین می‌کنند:<br>الف) آدرس‌های IP مبدأ (آدرس میزبان و آدرس شبکه)<br>ب) آدرس‌های IP مقصد (آدرس میزبان و آدرس شبکه)<br>پ) پورت مبدأ (TCP و UDP)<br>ت) پورت مقصد (TCP و UDP)<br>ث) پروتکل (IPv4 و IPv6)<br>ج) کد و نوع ICMP | |

| شماره الزام | نام الزام |
|---|---|
| ۳) به‌روزرسانی (وارد کردن) امضاها<br>۴) ایجاد امضاهای خاص<br>۵) پیکربندی کشف رفتارهای غیرعادی<br>۶) فعال‌سازی و غیر فعال‌سازی اقدامات هنگامی که امضا یا رفتارهای غیرعادی مورد شناسایی قرار می‌گیرند.<br>۷) تغییر آستانه‌هایی که واکنش‌های IPS را هدف می‌گیرند.<br>۸) تغییر مدت‌زمان بلوکه کردن ترافیک<br>۹) تغییر لیست سیاه و لیست سفید (از آدرس‌های IP و بازه آدرس‌ها)<br>۱۰) پیکربندی لیست سیاه و لیست سفید برای نادیده گرفتن خط‌مشی‌های IPS مبتنی بر امضا<br>[ | |

| شماره الزام | نام الزام |
|---|---|
| ۴۸ | **مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن** |
| محصول مورد ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست‌های امنیتی محدود کند.<br>**نکته کاربردی:**<br>این الزام امکان آغاز به‌روزرسانی دستی را به سرپرست محصول امنیتی محدود می‌کند. | |
| ۴۹ | **مدیریت داده‌های محصول ۱** |
| محصول مورد ارزیابی باید امکان «مدیریت» داده‌های توابع امنیتی محصول را به سرپرست‌های امنیتی محدود کند.<br>**نکته کاربردی:**<br>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 کردن. الزام حاضر همچنین شامل بازگرداندن گذرواژه کاربری به حالت پیش‌فرض توسط سرپرست محصول امنیتی است. عبارت "CoreData" در نام این الزام برای جداسازی آن با الزام ذکر شده در قسمت الزامات اختیاری با نام FMT_MTD.1/CryptoKeys است. | |
| ۵۰ | **کارکرد مدیریتی محصول ۱** |

| شماره الزام | نام الزام |
|---|---|

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

[اختصاص:

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

**نکته کاربردی:**

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

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

| شماره الزام | نام الزام |
|---|---|
| انتخاب کند. تغییر در مدیریت محصول، از «مستقیماً توسط سرپرستی راه دور» به «سرپرستی راه دور از طریق مؤلفه‌ی دیگر» می‌تواند به عنوان یک مثال برای پیکربندی تعاملات باشد. | |
| ۵۱ | **نقش‌های امنیتی ۳** |
| محصول باید نقش‌های زیر را نگهداری کند.<br>• سرپرست امنیتی | |
| ۵۲ | **نقش‌های امنیتی ۴** |
| محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار کند. | |
| ۵۳ | **نقش‌های امنیتی ۵** |
| محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند:<br>• نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را به صورت محلی اداره کند.<br>• نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را از راه دور اداره کند.<br>**نکته کاربردی:**<br>بر اساس این الزام سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک سازوکار راه دور اداره کند. نویسنده سند هدف ارزیابی باید الزامات FTP_ITC.1، FPT_ITT.1 و/یا FTP_TRP.1/Admin را برای اثبات چگونگی به دست آمدن یک ارتباط امن، انتخاب کند.<br>برای محصولات توزیع‌شده، نیاز نیست که هر مؤلفه مدیریت خود برای این الزام را پیاده‌سازی کند. حداقل یک مؤلفه باید احراز هویت و شناسایی سرپرستان امنیتی را بر اساس الزامات FIA_UIA_EXT.1 و FIA_UIA_EXT.2 پشتیبانی کند. برای اعمال شدن احراز هویت در دیگر مؤلفه‌ها، سرپرست امنیتی باید از طریق یک کانال امن (مطابق با الزامات FTP_ITC.1 یا FPT_ITT.1) و مؤلفه‌ای که احراز هویت و شناسایی را پشتیبانی می‌کند، با مؤلفه‌های دیگر ارتباط برقرار کند. شناسایی کاربرها و ارتباط بین کاربران و نقش‌ها نیز از طریق مؤلفه‌ای که احراز هویت و شناسایی را پشتیبانی می‌کند، انجام می‌گیرد. برای دیگر مؤلفه‌ها نیاز نیست که از سرپرستی محلی مؤلفه (ذکر شده در الزام FMT_SMR.2.3) پشتیبانی کنند. | |

### ۴,۷ کلاس حفاظت از محصول مورد ارزیابی

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

| شماره الزام | نام الزام |
|---|---|
| ۵۴ | **محافظت از داده‌های محصول (کلیدهای متقارن) ۱** |
| محصول مورد ارزیابی باید از خواندن تمام کلیدهایی که از پیش به اشتراک گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد.<br><br>**نکته کاربردی:**<br>هدف از الزام حاضر این 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. | |
| ۵۵ | **حفاظت از گذرواژه سرپرست محصول ۱** |
| محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند. | |
| ۵۶ | **حفاظت از گذرواژه سرپرست محصول ۲** |
| محصول مورد ارزیابی باید از خوانده شدن گذرواژه‌هایی که به‌صورت متن ساده[۱] هستند، جلوگیری کند.<br><br>**نکته کاربردی:**<br>هدف از الزام حاضر این است که داده‌های خام مربوط به احراز هویت از طریق گذرواژه، به شکل واضح ذخیره نشوند و هیچ کاربر و سرپرست محصول نتواند گذرواژه متن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصول که تمام دسترسی‌ها را داشته | |

[۱] Plaintext

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

### ۴,۷,۱ آزمون محصول مورد ارزیابی

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

| شماره الزام | نام الزام |
|---|---|
| **۵۷** | **خودآزمایی محصول ۱** |

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

**تذکر: در صورتی که برای خودآزمایی‌ها از سازوکار امضای دیجیتال استفاده شود نیاز است الزام «خودآزمایی محصول ۲» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه گردد.**

**نکته کاربردی:**

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

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

### ۴,۷,۲ به‌روزرسانی امن

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

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

| شماره الزام | نام الزام |
|---|---|
| ۵۸ | **به‌روزرسانی امن ۱** |
| محصول مورد ارزیابی باید این امکان را به سرپرستان امنیتی محصول بدهد که به نسخه فعلی نرم‌افزار/میان‌افزار محصول و [انتخاب: جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول، هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول] دسترسی داشته باشد.<br><br>**نکته کاربردی:** | |

| شماره الزام | نام الزام |
|---|---|
| | اگر امکان نصب یک به‌روزرسانی مورد اعتماد که همان لحظه فعال نمی‌گردد یعنی فعال‌سازی آن دارای تأخیر است، در محصول وجود داشته باشد، آنگاه باید هر دو نسخه محصول: نسخه مورد استفاده و نسخه نصب شده (به صورت تصویری از غیرفعال بودن آن) فراهم گردد. در این گونه موارد، گزینه «جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول» در انتخاب این الزام، باید منتخب گردد و همچنین در خلاصه مشخصات محصول باید مشخص گردد که چگونه و چه زمانی نسخه غیرفعال، فعال می‌گردد. اگر تمامی به‌روزرسانی‌ها هم‌زمان با نصب فعال می‌گردند، آنگاه فقط نسخه فعلی در حال اجرای محصول باید فراهم گردد و گزینه «هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول» برای انتخاب این الزام برگزیده خواهد شد.<br>برای محصولات توزیع‌شده، نحوه تصمیم‌گیری در رابطه با نسخه‌های نصب شده روی هر مؤلفه در سند راهنمای عملیاتی توضیح داده شده است. |
| **۵۹** | **به‌روزرسانی امن ۲** |
| | محصول مورد ارزیابی باید این امکان را برای سرپرستان امنیتی محصول فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار محصول مورد ارزیابی را به صورت دستی انجام دهد و [انتخاب: از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی‌های خودکار پشتیبانی کند، از هیچ سازوکار به‌روزرسانی دیگری پشتیبانی نکند].<br><br>**تذکر: در صورتی که نویسنده سند هدف امنیتی برای این الزام گزینه‌های به‌روزرسانی خودکار را انتخاب کند لازم است الزام «مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/به‌روزرسانی امن» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.**<br><br>**نکته کاربردی:**<br>عبارت «انتخاب» در این الزام، بین پشتیبانی از «جستجوی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز قائل می‌شود. «جستجوی خودکار به‌روزرسانی‌ها» به یک محصول مورد ارزیابی اشاره دارد که جستجو می‌کند تا ببیند به‌روزرسانی جدیدی وجود دارد یا خیر و این امر را به سرپرست محصول اطلاع می‌دهد (مثلاً از طریق یک پیام یا یک پرچم)، اما نصب به‌روزرسانی نیازمند انجام اقداماتی توسط سرپرست محصول خواهد بود، اما «به‌روزرسانی خودکار» به یک محصول مورد ارزیابی اشاره دارد که به‌روزرسانی‌ها را جستجو می‌کند و در صورت وجود آن‌ها را نصب می‌کند.<br>خلاصه مشخصات محصول باید بیان کند که چه اقداماتی برای پشتیبانی محصول از گزینه‌های «از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند» یا «از به‌روزرسانی‌های خودکار پشتیبانی کند» در قسمت «انتخاب» این الزام، دخیل هستند. |

| شماره الزام | نام الزام |
|---|---|
| | وقتی که برای حفاظت از سازوکار به‌روزرسانی مورد اعتماد، مقادیر هش‌شده منتشر شده است، محصول نباید به صورت خودکار فایل (ها) به‌روزرسانی به همراه مقدار هش را (ممکن است همراه فایل یا به صورت جدا از فایل باشد) دانلود کند و به صورت خودکار بدون هیچ‌گونه مجوز فعال[۱] از سرپرست امنیتی نصب کند، حتی برای مواردی که مقادیر محاسبه شده هش با مقادیر منتشر شده منطبق باشد. در این مورد نباید گزینه «از به‌روزرسانی‌های خودکار پشتیبانی کند» استفاده گردد (بررسی خودکار برای وجود به‌روزرسانی مانعی ندارد). در این گونه موارد باید همیشه یک مجوز فعال از سرپرست امنیتی وجود داشته باشد و گزینه «به‌روزرسانی دستی» باید انتخاب گردد، اگرچه ممکن است فایل (ها) به طور خودکار دانلود شده باشند.<br>به‌روزرسانی‌های کاملاً خودکار فقط باید در حالتی که از سازوکار امضاء دیجیتال استفاده شده باشد، انتخاب گردد. |
| ۶۰ | **به‌روزرسانی امن ۳** |
| | محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: سازوکار امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.<br><br>**تذکر: در صورتی که از سازوکار امضای دیجیتال استفاده شود نیاز است الزام‌های «الزامات به‌روزرسانی ۴» و «الزامات به‌روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.**<br><br>**نکته کاربردی:**<br>سازوکار امضاء دیجیتال که در این الزام به آن اشاره شده است، یکی از الگوریتم‌هایی است که در الزام «عملیات رمزنگاری ۱ (۲)» تشریح شده است. همچنین درهم‌ساز مورد استفاده در این الزام نیز توسط یکی از توابع تشریح‌شده در الزام «عملیات رمزنگاری ۱ (۳)» تولید می‌شود. نویسنده هدف امنیتی باید سازوکار اجرا شده توسط محصول مورد ارزیابی را تعیین کند، هر دو سازوکار نیز می‌تواند مورد استفاده قرار گیرد.<br>وقتی که از مقادیر هش منتشر شده برای امن کردن سازوکار به‌روزرسانی مورد اعتماد استفاده می‌شود، یک «مجوز فعال» برای فرآیند به‌روزرسانی، از طرف سرپرست امنیتی نیاز است. به علاوه، مخابره امن مقدار هش موثق[۲] از توسعه‌دهنده/تولیدکننده محصول به سرپرست امنیتی، یکی از فاکتورهای کلیدی برای حفاظت از سازوکار به‌روزرسانی مورد اعتماد است و سند راهنما باید چگونگی انجام این انتقال/مخابره را توضیح دهد. برای تصدیق[۳] مقدار هش مورد اعتماد توسط سرپرست امنیتی، چندین روش امکان‌پذیر است. |

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

| شماره الزام | نام الزام |
|---|---|
| سرپرست امنیتی می‌تواند مقدار هش را مانند فایل(ها) به‌روزرسانی به دست آورد و در حالی که هش کردن فایل(ها) در درون محصول در حال انجام است، تصدیق هش را خارج از محصول انجام دهد.<br>وقتی تصدیق هش موفق باشد، محصول می‌تواند بدون هیچ گام اضافه دیگری از طرف سرپرست امنیتی، به‌روزرسانی را انجام دهد. احراز هویت شدن به عنوان سرپرست امنیتی و فرستادن مقدار هش به محصول معادل با «مجوز فعال» برای به‌روزرسانی امن، در نظر گرفته می‌شود (وقتی تصدیق هش با موفقیت انجام شود)، زیرا انتظار می‌رود وقتی که به‌روزرسانی مدنظر باشد، سرپرست مقدار هش را روی محصول بارگذاری کند.<br>اگر سازوکار امضاء دیجیتال انتخاب گردد، تصدیق امضاء به‌وسیله خود محصول انجام می‌گیرد. برای سازوکار هش منتشرشده، تصدیق هم به‌وسیله سرپرست امنیتی و هم محصول قابل انجام است.<br>برای محصولات توزیع شده، همه مؤلفه‌ها باید از به‌روزرسانی امن پشتیبانی کنند. تصدیق امضاء یا هش به‌روزرسانی، باید به‌وسیله هر مؤلفه محصول (تصدیق امضاء) یا برای هر مؤلفه محصول (تصدیق هش) انجام گیرد.<br>**نکته کاربردی**:<br>در نسخه‌های بعدی این پروفایل حفاظتی، لازم خواهد شد که برای به‌روزرسانی‌های امن، از یک سازوکار امضاء دیجیتال استفاده شود.<br>**نکته کاربردی:**<br>اگر در سازوکار تائید به‌روزرسانی از گواهی‌نامه‌ها استفاده شود، این گواهی‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب شده و بر اساس «الزامات پروتکل X509» تائید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی ۲» باید در سند هدف امنیتی در نظر گرفته شود.<br>**نکته کاربردی:**<br>در این الزام کارکرد امنیتی، منظور از «به‌روزرسانی»، فرایند جایگزین کردن یک مؤلفه نرم‌افزاری غیر فرار (non-volatile) با یک مؤلفه دیگر است. به مؤلفه اول، تصویر غیر فرار یا تصویر NV و به مؤلفه دوم، تصویر به‌روزرسانی گفته می‌شود. هر چند که تصویر به‌روزرسانی معمولاً جدیدتر از تصویر NV است، اما الزامی در این زمینه وجود ندارد. در مواردی ممکن است مالک سیستم بخواهد آن را به نسخه قدیمی‌تر برگرداند و این کار ایرادی ندارد (مثلاً هنگامی که شرکتی یک به‌روزرسانی معیوب را منتشر کند، یا هنگامی که سیستم مبتنی بر کارکرد یک ویژگی مستندسازی نشده، باشد که در به‌روزرسانی جدید وجود ندارد). همچنین، ممکن است مالک سیستم بخواهد به‌روزرسانی را با تصویر NV انجام دهد تا معایب موجود را برطرف کند. | |

| 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 سازوکار به‌روزرسانی تائید 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 تائید از طریق مقایسه کلیدهای عمومی) یا امضاشده توسط کلیدهای امضای معتبر را تائید کند (مثلاً تائید گواهی‌نامه‌ها در صورت استفاده از گواهی‌نامه‌های X.509). | |
| ۶۱ | **مهرهای زمانی ۱** |
| محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان[۲] برای استفاده خودش را داشته باشد. | |
| ۶۲ | **مهرهای زمانی ۲** |
| محصول باید [انتخاب: به سرپرست امنیتی اجازه دهد که زمان را تنظیم کند، زمان را با منابع خارجی زمان همگام سازد].<br>**نکته کاربردی:**<br>مهرهای زمانی قابل‌اطمینان جهت استفاده با دیگر توابع امنیتی محصول، مورد نظر می‌باشند؛ به عنوان مثال، برای تولید داده ممیزی جهت اجازه دادن به سرپرست امنیتی که بتواند با بررسی کردن ترتیب رویدادها، وقایع را بازنگری کند و زمان واقعی که وقایع رخ داده است را تعیین کند. تصمیم در مورد سطح دقت اطلاعات (از لحاظ میزان دقیق بودن زمان رویدادها) به عهده سرپرست است. محصول به اطلاعات خارجی زمان و تاریخ وابسته است، این اطلاعات می‌تواند به صورت دستی توسط سرپرست امنیتی تهیه گردند یا به وسیله استفاده از یک یا چند منبع خارجی مانند سرور NTP به دست آورده شوند؛ بنابراین گزینه مناسب در «انتخاب» این الزام باید برگزیده شود. استفاده از یک ساعت بلادرنگ محلی با قابلیت همگام‌سازی خودکار با یک منبع خارجی (مثلاً؛ سرور NTP) توصیه می‌گردد، ولی الزام نیست. همچنین برای ارتباط با یک منبع خارجی، استفاده از الزام FTP_ITC.1 اختیاری است ولی نویسنده سند هدف امنیتی باید مشخص سازد که چگونه اطلاعات زمان و تاریخ به‌وسیله محصول دریافت و نگهداری می‌گردد.<br>عبارت «مهرهای زمانی قابل‌اطمینان» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ناپیوسته ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده ممیزی را محاسبه کرد. | |

[۱] Firmware

[۲] Reliable time stamps

| شماره الزام | نام الزام |
|---|---|
| توجه شود که تمامی تغییرات ناپیوسته زمان؛ به‌وسیله سرپرست یا به صورت خودکار توسط فرآیند، باید ممیزی گردد. اگر زمان به‌وسیله هسته یا خود سیستم تغییر کند، نیاز به ممیزی نیست، این تغییرات دیگر در حوزه تغییرات ناپیوسته زمان، قرار نمی‌گیرند. | |

### ۴,۸ 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. سرپرستان باید قادر باشند نشست‌های تعاملی خود را خاتمه دهند. در ابتدای هر نشست باید یک اطلاعیه مشاوره‌ای برای آن‌ها نمایش داده شود.

| شماره الزام | نام الزام |
|---|---|
| ۶۳ | **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:<br>• 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 کند؛<br>• نشست را خاتمه دهد]. | |
| ۶۴ | **قفل‌کردن و خاتمه دادن به نشست‌ها ۵** |
| در مورد نشست‌های تعاملی راه دور[۲]، در صورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت‌زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود. | |

[۱] Local interactive sessions

[۲] Remote

| شماره الزام | نام الزام |
|---|---|
| ۶۵ | **قفل‌کردن و خاتمه دادن به نشست‌ها ۶** |
| محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد. | |
| ۶۶ | **پیغام‌های هشدار در رابطه با استفاده محصول ۱** |
| قبل از ایجاد یک نشست کاربری سرپرست اجرایی[۱]، محصول مورد ارزیابی باید توصیه‌های مشخص شده توسط سرپرست امنیتی و همچنین تأییدیه استفاده از محصول مورد ارزیابی را نشان دهد.<br>**نکته کاربردی:**<br>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. | |

### ۴,۹ 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 پنج پروتکل استاندارد ایجاد می‌شوند: IPsec, TLS, DTLS, HTTPS و SSH. این پروتکل‌ها توسط RFC هایی تعیین می‌شوند که گزینه‌های پیاده‌سازی مختلفی را در اختیار کاربران قرار می‌دهند. در مورد برخی از این گزینه‌ها الزاماتی نیز جود دارد (مخصوصاً گزینه‌های مربوط به مقادیر اولیه رمزنگاری). هدف این است که قابلیت همکاری و مقاومت در برابر حملات رمزنگاری افزایش یابد. این پروتکل‌ها علاوه بر حفاظت در برابر افشای اطلاعات (و شناسایی تغییرات ایجادشده)، امکان 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 |
|---|---|
| ۶۷ | **کانال امن ۱** |

[۱] Administrative user

| شماره الزام | نام الزام |
|---|---|
| محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احراز هویت، اختصاص: [دیگر قابلیت‌ها]، هیچ قابلیت‌های دیگری] که به طور منطقی از کانال‌های دیگر متمایز است فراهم کند تا آن‌ها را احراز هویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت کرده و تغییرات را تشخیص دهد.<br><br>**تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH، DTLS،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.** | |
| **۶۸** | **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. | |
| **۶۹** | **کانال امن ۳** |
| محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: لیست سرویس‌های که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی کند.<br>**نکته کاربردی:**<br>هدف از الزام حاضر فراهم کردن روشی است که جهت حفاظت ارتباطات خارجی با موجودیت‌های معتبر IT، از پروتکل رمزنگاری استفاده گردد. منظور از موجودیت‌های معتبر IT، موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست‌کم از یکی از پروتکل‌های ذکر شده در الزام «کانال امن ۱» استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی، ارتباط برقرار کند. اگر ارتباط با یک سرور احراز هویت (مانند؛ RADIUS) برقرار شود، نویسنده هدف امنیتی باید عبارت «سرور احراز هویت» را در دومین «انتخاب» الزام «کانال امن ۱» انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های ذکر شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی را انجام دهد و موارد مناسب را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی سازوکار یا سازوکارهای پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌کند که الزامات پروتکل در پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند.<br>هر چند که هیچ الزامی در مورد طرف آغازکننده ارتباط وجود ندارد، نویسنده هدف امنیتی در عبارت اختصاص این الزام، سرویس‌های که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباط با موجودیت IT معتبر آغاز کند را لیست می‌کند.<br>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. | |

| شماره الزام | نام الزام |
|---|---|
| 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. | |
| ۷۰ | **مسیر امن ۱** |
| محصول، باید با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] مسیر ارتباطی امنی را میان خود و سرپرست‌های راه دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم کند و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت کرده و تغییرات در داده کانال را تشخیص دهد.<br>**تذکر: در صورتی که هر یک از پروتکل‌های HTTPS،TLS،DTLS،SSH،IPsec به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.** | |
| ۷۱ | **مسیر امن ۲** |
| محصول مورد ارزیابی باید به سرپرست‌های راه دور محصول اجازه دهد که ارتباطات را از طریق کانال امن آغاز کند. | |
| ۷۲ | **مسیر امن ۳** |
| محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه سرپرست محصول و تمام فعالیت‌های راه دور سرپرستی الزامی کند.<br>**نکته کاربردی:**<br>این الزام اطمینان حاصل می‌کند که سرپرست‌های راه دور مجاز، تمام ارتباطات با محصول مورد ارزیابی را، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌کنند. داده‌های منتقل شده از طریق این مسیر، با استفاده از پروتکل انتخاب‌شده در عبارت «انتخاب»، رمزگذاری می‌شوند. نویسنده سند هدف امنیتی، سازوکار یا سازوکارهای پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌کند که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند. | |

### ۴,۱۰ کلاس IPS: جلوگیری از نفوذ

| شماره الزام | نام الزام |
|---|---|
| ۷۳ | **کارکرد IPS مبتنی بر رفتار غیرعادی ۱** |

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

[انتخاب:

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

و فیلدهای پروتکل شبکه زیر:

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

**نکته کاربردی:**

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

تناوب را می‌توان چنین تعریف کرد: تعداد دفعات وقوع هر رویداد (مثل شناسایی بسته‌هایی که مطابق با یک امضا هستند) طی یک بازه مشخص زمانی، مانند تعداد نشست‌های FTP که طی یک ساعت ایجاد می‌شوند. اگر «تناوب‌ها» انتخاب شوند، «خلاصه مشخصات محصول» باید توضیحی از نحوه تعریف تناوب‌ها در محصول ارائه کند.

آستانه‌ها را می‌توان این‌گونه تعریف کرد: میزان یا درصد انحراف از مرزها یا سطوح مورد انتظار، مثل تعداد مگابایت‌هایی که هر ساعت از FTP عبور می‌کنند. اگر «آستانه‌ها» انتخاب شود، «خلاصه مشخصات محصول» باید توضیحی از نحوه تعریف آستانه‌ها در محصول ارائه کند.

| ۷۴ | **کارکرد IPS مبتنی بر رفتار غیرعادی ۲** |
|---|---|

محصول باید از تعریف فعالیت غیرعادی از طریق: [انتخاب: پیکربندی دستی توسط سرپرست، پیکربندی خودکار] پشتیبانی کند.

[۱] Baselines

[۲] Throughput

**نکته کاربردی:**
مبنا و ناهنجاری گاهی می‌توانند به صورت دستی توسط سرپرست محصول، پیکربندی/تعیین شوند، یا چیزی که محصول بتواند آن را به صورت خودکار با بازرسی ترافیک شبکه طی بازه زمانی مشخص، تعریف/ایجاد کند (به این کار پروفایلینگ نیز گفته می‌شود). لازم نیست که محصول IPS قابلیت «پروفایلینگ» شبکه را داشته باشد تا مبنا یا قاعده‌ای را به صورت پویا تعریف کند و اگر محصول IPS این کارکرد را داشته باشد، چنین کارکردی به عنوان بخشی از بسته تکمیلی IPS مورد ارزیابی قرار نمی‌گیرد.

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

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

- در هر حالتی، برای هر واسط حسگری: [انتخاب:
  - اجازه به جریان ترافیک
  - ارسال یک بازنشانی TCP به آدرس مبدأ ترافیک متخلف
  - ارسال یک بازنشانی TCP به آدرس مقصد ترافیک متخلف
  - ارسال یک پیام غیرقابل دسترسی ICMP [انتخاب‌ها: میزبان، مقصد، پورت]
  - هدف‌گیری یک ابزار شبکه غیر محصول برای بلوکه کردن الگوی ترافیک متخلف]
- در حالت درون‌خطی:
  - اجازه به جریان ترافیک
  - بلوکه کردن/ قطع جریان ترافیک

و [انتخاب: اصلاح و ارسال بسته‌ها قبل از اینکه از محصول عبور کنند، بدون هیچ اقدام دیگر]

| ۷۶ | **بلوکه کردن آدرس IP ۱** |
|---|---|

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

**نکته کاربردی:**
نوع آدرس‌هایی که در این تابع هدف امنیتی تعریف شده است، محدود است به آدرس‌های IP (مثل یک آدرس IP واحد یا بازه‌ای از آدرس‌های IP) زیرا این بسته تکمیلی IPS، به بازرسی ترافیک IP محدود است. هدف‌های ارزیابی از نوع IPS از فعال‌سازی کارکردهایی که جریان ترافیک را بر اساس انواع دیگر آدرس (مثل MAC) متوقف/ مجاز کنند، جلوگیری نمی‌کند؛ اما زمانی که از این کارکرد

| | |
|---|---|
| استفاده می‌شود، مستندات دستورالعمل‌ها و «خلاصه مشخصات محصول» باید شرح دهند که چه نوع پیکربندی باعث ایجاد لیست آدرس‌های سفید و سیاه غیر IP شده‌اند تا بر لیست آدرس‌های مبتنی بر IP اولویت یابد. | |
| **۷۷** | **بلوکه کردن آدرس IP ۲** |
| محصول باید به سرپرست IPS و [انتخاب: هیچ نقش دیگر [الزام: نقش‌های دیگر]] اجازه دهد که عناصر خط‌مشی IPS را پیکربندی کند (قوانین لیست سیاه، قوانین لیست سفید، آدرس‌های IP). | |
| **۷۸** | **تحلیل ترافیک شبکه ۱** |
| محصول باید ترافیک شبکه مبتنی بر IP را که به واسط‌های حس‌گر محصول جریان دارد، تجزیه و تحلیل کند و نقض خط‌مشی‌هایی را که توسط سرپرست تعریف شده است، شناسایی کند.<br><br>**نکته کاربردی:**<br>اگرچه ممکن است در برخی محصولات، هر واسط محصول بتواند به عنوان واسط حس‌گر عمل کند، ولی این موارد مورد نظر نمی‌باشند. در این الزام اصطلاح «واسط حس‌گر» برای هر واسط محصول که یک یا چند خط‌مشی IPS روی آن اعمال شده است، استفاده می‌شود. یک خط‌مشی IPS سرپرستی تعریف‌شده، به هر مجموعه‌ای از قوانین برای تحلیل ترافیک، مسدودسازی ترافیک، تشخیص امضاء و/یا تشخیص ناهنجاری اعمال شده بر روی یک یا چند واسط حس‌گر، گفته می‌شود. محصول ممکن است قادر باشد به سرپرست اجازه دهد که اولویت المان‌های خط‌مشی امنیتی (لیست سیاه و سفید، قوانین مبتنی بر امضاء و قوانین مبتنی بر ناهنجاری) را پیکربندی کند، ولی چنین پیکربندی‌هایی در این سند الزام نمی‌باشند. | |
| **۷۹** | **تحلیل ترافیک شبکه ۲** |
| محصول باید پروتکل‌های ترافیک شبکه زیر را پردازش کند (بتواند بازرسی کند):<br>• پروتکل اینترنت (IPv4)، RFC 791<br>• پروتکل اینترنت نسخه ۶ (IPv6)، RFC 2460<br>• پروتکل پیام کنترل اینترنت نسخه ۴ (ICMPv4)، RFC 792<br>• پروتکل پیام کنترل اینترنت نسخه ۶ (ICMPv6)، RFC 2463<br>• پروتکل کنترل انتقال (TCP)، RFC 793<br>• پروتکل داده‌های کاربر (UDP)، RFC 768 | |

**نکته کاربردی:**

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

| ۸۰ | **تحلیل ترافیک شبکه ۳** |
|---|---|

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

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

**نکته کاربردی:**

انواع واسط‌ها ممکن است اترنت، گیگابیت اترنت و غیره باشد. واسط‌های بی‌قاعده، واسط‌هایی هستند که ترافیک شبکه را به منظور بازرسی شبکه شنود می‌کنند، اما هیچ کارکردی در لایه‌های ۲،۳ و بالاتر فراهم نمی‌آورند؛ بنابراین سرویس‌های شبکه بر روی واسط‌ها شنود نمی‌شوند و هیچ پشته پروتکل IP بر روی واسط فعال نیست، در نتیجه هیچ آدرس IP به واسطی اختصاص داده نمی‌شود. واسط‌های درون‌خط، جفت واسط‌هایی هستند که مسیری را برای ترافیک شبکه فراهم می‌آورند به‌طوری‌که بتوان جریان شبکه را بلوکه و یا توسط محصول ویرایش کرد. واسط‌های بی‌قاعده و درون‌خط کارکردهای لایه ۳ و بالاتر را پشتیبانی نمی‌کنند، آن‌ها ممکن

[۱] Promiscuous

| |
|---|
| است کارکردهای لایه ۲ را فراهم کنند (با آدرس فیزیکی نسبت داده شده به واسطها) تا اجازه دهند دستگاه‌های شبکه، ترافیک شبکه را به محصول ارسال و یا دریافت کنند. |
| **۸۱** \| **کارکرد IPS مبتنی بر امضاء ۱** |
| محصول باید از بازرسی محتوای سرآیند بسته‌ها پشتیبانی کند و بتواند حداقل سرآیند فیلدهای زیر را بازرسی کند:<br>• IPv4: نسخه، طول سرآیند، طول بسته، پرچم IP، ID، آفست تکه[۱]، زمان فعالیت (TTL)، پروتکل، سرآیند checksum، آدرس مبدأ، آدرس مقصد، گزینه‌های IP و[ انتخاب: نوع سرویس (ToS)، هیچ فیلد دیگری] .<br>• IPv6: نسخه، طول محتوا، سرآیند بعدی، محدودیت گام، آدرس مبدأ، آدرس مقصد، سرآیند مسیریاب و[ انتخاب: کلاس ترافیک، برچسب جریان، هیچ فیلد دیگری] .<br>• ICMP: نوع، کد، checksum سرآیند و [انتخاب: ID، شماره توالی، [اختصاص: سایر فیلدها در سرآیند ICMP ]]<br>• ICMPv6: نوع، کد و checksum سرآیند<br>• TCP: پورت مبدأ، پورت مقصد، عدد توالی، عدد تصدیق، آفست، رزرو، پرچم‌های TCP، پنجره، checksum، نشانگر اضطراری و گزینه‌های TCP<br>• UDP: پورت مبدأ، پورت مقصد، طول و UDP checksum |
| **۸۲** \| **کارکرد IPS مبتنی بر امضاء ۲** |
| محصول باید از بازرسی محتوای سرآیند بسته‌های پشتیبانی کند و قادر باشد حداقل فیلدهای سرآیند زیر را بازرسی کند تا فرایند تطابق الگوهای مبتنی بر رشته‌های داده را اجرا کند:<br>• داده‌های ICMPv4: کاراکترهایی بیشتر از ۴ بیت اول از سرآیند ICMP<br>• داده‌های ICMPv6: کاراکترهایی بیشتر از ۴ بیت اول از سرآیند ICMP<br>• داده‌های TCP (کاراکترهایی بیشتر از ۲۰ بیت سرآیند TCP)، با پشتیبانی برای شناسایی:<br>- دستورات FTP (انتقال فایل): help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, type.<br>- دستورات و محتوای HTTP (وب): دستوراتی شامل GET و POST و رشته‌های تعیین‌شده توسط سرپرست مطابق با URL/URI ها و محتوای صفحه وب.<br>- وضعیت SMTP (ایمیل): شروع وضعیت، وضعیت دستورات SMTP، وضعیت سرآیند mail، وضعیت بدنه mail، وضعیت قطع فرایند. |

[۱] Fragment

- [انتخاب: [اختصاص: دیگر انواع بازرسی محتوای TCP]
- داده UDP: کاراکترهایی بیشتر از هشت بیت اول سرآیند UDP
- [اختصاص: دیگر انواع بازرسی محتوای بسته‌ها]

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

| ۸۳ | **کارکرد IPS مبتنی بر امضاء ۳** |
|---|---|

محصول باید قادر به کشف امضاهای مبتنی بر سرآیند (با استفاده از فیلدهای مشخص شده در IPS_SBD_EXT.1.1) در واسط‌های حسگر IPS باشد.

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

| ۸۴ | **کارکرد IPS مبتنی بر امضاء ۴** |
|---|---|

توابع امنیتی محصول باید بتواند تمامی امضاهای کشف الگوی ترافیکی زیر را شناسایی کند و این امضاها را در واسط حسگر IPS به کار گیرد:

- سیل‌آسا به میزبان (حمله DoS)
  - سیل‌آسا ICMP (حمله Smurf، سیل‌آسا ping)

- سیل‌آسا TCP (مثل سیل‌آسا SYN)
- سیل‌آسا به شبکه (حمله DoS)
- اسکن پورت و پروتکل (حملات شناسایی که آدرس‌های IP را برای یافتن سرویس‌های باز/ فعال/ در حال شنیدن اسکن می‌کنند).
  - اسکن پروتکل IP
  - اسکن پورت TCP
  - اسکن پورت UDP
  - اسکن ICMP

**نکته کاربردی:**

این الزام حداقل مجموعه از فیلدهای بسته سرآیند، رشته‌های بسته بار، انواع امضاء و الگوهای ترافیک بدخواه بالقوه (مانند سیل‌آسا و پویش) که محصول باید تشخیص دهد را، تعریف می‌کند. امضاهای معتبر ممکن است با یک، برخی و یا همه مشخصه‌های بیان شده در این الزام تطابق یابد و همچنین محصولات IPS ممکن است مشخصه‌های بیشتری نسبت به آنچه لیست شده است را جهت بررسی، پشتیبانی کنند ولی فقط موارد لیست شده در این الزام باید توسط ارزیاب‌ها مورد آزمون قرار گیرند. مجموعه مشخصه‌های، انواع امضاها، الگوهای ترافیک و غیره؛ که در الزام ذکر شده است، به منظور شناسایی کامل فعالیت‌های بدخواهانه یا حملات DDoS نیست. هدف از این الزام پوشش حملاتی است که از یک آدرس IP صورت می‌گیرد.

پویش پورت و پروتکل، به شناسایی حملاتی که با هدف قرار دادن چندین پورت/پروتکل بر روی یک یا چند آدرس IP، هدف را برای سرویس‌های باز/پاسخگو و ... پویش می‌کند، اشاره دارد.

| ۸۵ | **کارکرد IPS مبتنی بر امضاء ۵** |
|---|---|

محصول به عملیات زیر اجازه می‌دهد تا با خط‌مشی‌های IPS مبتنی بر امضا، ترکیب شوند:

- در هر حالتی، برای هر واسط حسگر: [انتخاب:
  - اجازه به جریان ترافیک
  - ارسال بازنشانی TCP به آدرس مبدأ ترافیک متخلف
  - ارسال بازنشانی TCP به آدرس مقصد ترافیک متخلف
  - ارسال پیام غیرقابل دسترسی ICMP انتخاب: میزبان، مقصد، پورت
  - هدف‌گیری یک ابزار شبکه غیر محصول برای بلوکه کردن الگوی ترافیک متخلف]
- حالت بر خط
  - اجازه به جریان ترافیک

- بلوکه کردن/ قطع جریان ترافیک
- و [انتخاب: اصلاح و ارسال بسته‌ها قبل از اینکه از محصول عبور کنند، بدون هیچ اقدام دیگری]

# ۵ الزامات تضمین امنیت

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

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

## ۵,۱ کلاس توسعه

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

### ۵,۱,۱ مشخصات کارکردی

مشخصات کارکردی، واسط‌های کارکرد امنیتی محصول را توصیف می‌کند 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 ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مشخصات کارکردی را ارائه کند. |
| | **نام عنصر: مشخصات کارکرد ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند.<br>**نکته کاربردی:**<br>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** |
| | **نام عنصر: مشخصات کارکرد ابتدایی ۱** |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مشخصات کارکردی **(ADV_FSP)** | **شماره مؤلفه: (ADV_FSP.1.1C)**<br>**شرح مؤلفه:**<br>مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی[۱] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲] توصیف کند. |
| | **نام عنصر: مشخصات کارکرد ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.2C)**<br>**شرح مؤلفه:**<br>مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص کند. |
| | **نام عنصر: مشخصات کارکرد ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.3C)**<br>**شرح مؤلفه:**<br>مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه کند. |
| | **نام عنصر: مشخصات کارکرد ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.4C)**<br>**شرح مؤلفه:**<br>ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد. |

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

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مشخصات کارکردی **(ADV_FSP)** | **نام عنصر: مشخصات کارکرد ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند. |
| | **نام عنصر: مشخصات کارکرد ابتدایی ۱**<br>**شماره مؤلفه: (ADV_FSP.1.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید مشخص کند 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.

### ۵,۲ کلاس راهنمای کاربر

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

### ۵,۲,۱ راهنمای کاربردی

| مؤلفه‌های اقدامات توسعه‌دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای کاربردی **(AGD_OPE)** | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید راهنمای کاربردی ارائه کند. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای کاربردی **(AGD_OPE)** | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.1C)**<br>**شرح مؤلفه:**<br>سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف کند، همانند هشدارهای مناسب. |
| | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.2C)**<br>**شرح مؤلفه:**<br>سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد. |
| | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.3C)**<br>**شرح مؤلفه:**<br>سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف کرده و مقادیر امن را به صورت مناسبی تعیین کند. |

| مؤلفه‌های محتوایی | |
|---|---|
| نام خانواده | عنصر امنیتی |
| | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.4C)**<br>**شرح مؤلفه:**<br>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 کند، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول. |
| | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.5C)**<br>**شرح مؤلفه:**<br>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 کنند. |
| | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.6C)**<br>**شرح مؤلفه:**<br>سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند. |
| | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.7C)**<br>**شرح مؤلفه:**<br>سند راهنمای کاربردی باید واضح و قابل‌فهم باشد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای کاربردی **(AGD_OPE)** | **نام عنصر: راهنمای کاربردی ۱**<br>**شماره مؤلفه: (AGD_OPE.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌کند. |

### ۵,۲,۲ راهنمای آماده‌سازی

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

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای آماده-سازی **(AGD_PRE)** | **نام عنصر: راهنمای آماده‌سازی ۱**<br>**شماره مؤلفه: (AGD_PRE.1.1C)**<br>**شرح مؤلفه:**<br>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**<br>**شماره مؤلفه: (AGD_PRE.1.2C)** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شرح مؤلفه:**<br>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**<br>**شماره مؤلفه: (AGD_PRE.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند. |
| | **نام عنصر: راهنمای آماده‌سازی ۱**<br>**شماره مؤلفه: (AGD_PRE.1.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید کند، محصول می‌تواند به صورت امن برای عمل کردن آماده شود. |

## ۵,۳ 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.

### ۵,۳,۱ 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 می‌باشد. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند کند.

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

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

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| آزمون مستقل **(ATE_IND)** | **نام عنصر: آزمون مستقل ۱**<br>**شماره مؤلفه: (ATE_IND.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌کند. |
| | **نام عنصر: آزمون مستقل ۱**<br>**شماره مؤلفه: (ATE_IND.1.2E)** |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| | **شرح مؤلفه:**<br>ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون کند تا تائید کند که توابع امنیتی محصول به صورت مشخص شده عمل می‌کنند. |

## ۵,۴ کلاس آسیب‌پذیری

### ۵,۴,۱ تحلیل آسیب‌پذیری

| مؤلفه‌های اقدامات توسعه‌دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آسیب‌پذیری **(AVA_VAN)** | **نام عنصر: آسیب‌پذیری ۱**<br>**شماره مؤلفه: (AVA_VAN.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید برای آزمودن، محصول را ارائه کند. |

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

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آسیب‌پذیری **(AVA_VAN)** | **نام عنصر: آسیب‌پذیری ۱**<br>**شماره مؤلفه: (AVA_VAN.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌کند. |
| | **نام عنصر: آسیب‌پذیری ۱**<br>**شماره مؤلفه: (AVA_VAN.1.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد. |
| | **نام عنصر: آسیب‌پذیری ۱**<br>**شماره مؤلفه: (AVA_VAN.1.3E)**<br>**شرح مؤلفه:**<br>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 کند. |

## ۵,۵ کلاس پشتیبانی از چرخه حیات

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

### ۵,۵,۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (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**<br>**شماره مؤلفه: (ALC_CMC.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید محصول و مرجع محصول را ارائه کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| قابلیت‌های پیکربندی **(ALC_CMC)** | **نام عنصر: برچسب‌گذاری محصول ۱**<br>**شماره مؤلفه: (ALC_CMC.1.1C)**<br>**شرح مؤلفه:**<br>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**<br>**شماره مؤلفه: (ALC_CMC.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند. |

### ۵,۵,۲ حوزه پیکربندی

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

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| حوزه پیکربندی **(ALC_CMS)** | **نام عنصر: پوشش پیکربندی محصول ۱**<br>**شماره مؤلفه: (ALC_CMS.1.1C)**<br>**شرح مؤلفه:**<br>لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد. |
| | **نام عنصر: پوشش پیکربندی محصول ۱**<br>**شماره مؤلفه: (ALC_CMS.1.1C)**<br>**شرح مؤلفه:**<br>لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی کند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| حوزه پیکربندی **(ALC_CMS)** | **نام عنصر: پوشش پیکربندی محصول ۱**<br>**شماره مؤلفه: (ALC_CMS.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند. |

## ۶ پیوست یک: الزامات اختیاری

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

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

### ۶,۱ کلاس ممیزی امنیت

درصورتی‌که در محصول مورد ارزیابی فضای حافظه محلی برای داده‌های ممیزی در نظر گرفته شده باشد، محصول مورد ارزیابی می‌تواند ادعا کند که مطابق آنچه در «ذخیره‌سازی رویدادهای ممیزی» گفته شده است، از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری به عمل آورد. فضای حافظه محلی دستگاه‌های شبکه برای ذخیره‌سازی داده‌های ممیزی، محدود است. اگر این حافظه پر شود، امکان از دست رفتن داده‌های ممیزی وجود خواهد داشت. ممکن است یک سرپرست محصول بخواهد اطلاعات مربوط به تعداد داده‌های ممیزی ازدست‌رفته را داشته باشد. این تعداد می‌تواند نشان‌دهنده مشکلات سرور باشد؛ بنابراین، «محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی» و «ذخیره‌سازی رویدادهای ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی» تهیه شده‌اند تا این قابلیت‌های اختیاری دستگاه‌های شبکه را بیان کنند.

همچنین جدول زیر مربوط به رویدادهای ممیزی الزامات اختیاری 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 ثبت‌شده |
|---|---|---|---|
| ۱. | ذخیره‌سازی رویدادهای ممیزی ۱ و ۲ | | |
| ۲. | محل ذخیره‌سازی داده‌های ممیزی ۳ / فضای ذخیره‌سازی ممیزی محلی | | |
| ۳. | ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی | کم بودن فضای ذخیره‌سازی برای رویدادهای ممیزی. | |
| ۴. | الزامات پروتکل X509(۱) و (۲)/ تبادل داده کاربردی داخل محصول | تلاش‌های ناموفق برای اعتبارسنجی یک گواهی‌نامه. | دلیل/دلایل شکست |
| ۵. | مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها | آغاز و توقف سرویس‌ها. | |
| ۶. | مدیریت داده‌های محصول ۱/ کلیدهای رمزنگاری | مدیریت کلیدهای رمزنگاری. | |
| ۷. | انتقال داده امنیتی در داخل محصول ۱ | راه‌اندازی اولیه و خاتمه دادن به کانال مورد اعتماد.<br>شکست توابع کانال مورد اعتماد. | شناسایی آغازکننده و هدفی که تلاش در برقراری کانال‌های مورد اعتماد با آن/برای آن شکست‌خورده است |
| ۸. | مسیر امن ۱، ۲ و ۳/ پیوند زدن | راه‌اندازی اولیه و خاتمه دادن به مسیر مورد اعتماد.<br>شکست توابع مسیر مورد اعتماد. | |
| ۹. | | فعال‌سازی و غیر فعال‌سازی ارتباطات مابین یک جفت از مؤلفه‌ها. | هویت‌های جفت نقاط انتهایی[۱] فعال یا غیرفعال شده |

[۱] Endpoints pairs

**نکته کاربردی:**

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

- وجود افزونه basicConstraints و تائید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تائید 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 کرد.

| شماره الزام | نام الزام |
|---|---|
| ۸۶ | **ذخیره‌سازی داده‌های ممیزی ۱** |
| محصول مورد ارزیابی باید از پاک شدن غیرمجاز داده‌های ممیزی جلوگیری کند. | |
| ۸۷ | **ذخیره‌سازی داده‌های ممیزی ۱** |
| محصول مورد ارزیابی باید از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری کند. | |
| ۸۸ | **محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی** |

محصول مورد ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده‌های ممیزی [انتخاب: از بین رفته، بازنویسی شده را، [اختصاص: سایر اطلاعات]] ارائه کند. محصول مورد ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده‌های ممیزی ۳» را انجام می‌دهد.

**نکته کاربردی:**

این گزینه باید انتخاب گردد، در صورتی که محصول مورد ارزیابی از این کارکرد پشتیبانی کند.

درصورتی‌که حافظه محلی داده‌های ممیزی توسط سرپرست محصول خالی شود، شمارنده‌های مربوط به انتخاب انجام‌شده باید به مقادیر اولیه خود برگردند (این مقدار در اکثر موارد صفر است). سند راهنما باید به سرپرست محصول هشدار دهد که خالی کردن حافظه ممکن است سبب از دست رفتن داده‌ها شود.

برای محصولات توزیع‌شده، هر مؤلفه که از دست رفتن داده ممیزی را شمارش می‌کند باید سازوکاری را برای سرپرست فراهم آورد که امکان دسترسی به اطلاعات و مدیریت اطلاعات داشته باشد.

| |
|---|
| اگر این الزام در سند هدف امنیتی بیان گردد آنگاه نویسنده سند هدف امنیتی باید به صورت واضح هر شرایطی را که در آن شمارش از دست رفتن ممیزی انجام نمی‌گیرد، توضیح دهد. |
| **۸۹** \| **ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی** |
| در صورتی که حجم داده‌های ممیزی از ظرفیت ذخیره‌سازی محلی داده‌های ممیزی فراتر رود/سرریز کند، محصول مورد ارزیابی باید با تولید اخطار، سرپرست را آگاه کند.<br>**نکته کاربردی:**<br>این گزینه باید انتخاب گردد، درصورتی‌که محصول مورد ارزیابی امکان تولید پیام برای سرپرست را وقتی حافظه محلی در نظر گرفته شده برای داده ممیزی پر می‌شود، داشته باشد. درصورتی‌که داده‌های مربوط به رویدادهای قابل‌ممیزی تنها در حافظه محلی ذخیره شده باشند، این هشدار می‌تواند اهمیت بسیار زیادی داشته باشد.<br>باید اطمینان حاصل کرد که هشدار مورد اشاره در «محل ذخیره‌سازی داده‌های ممیزی ۳» را می‌توان به اطلاع سرپرست رساند. از آنجایی که نمی‌توان تضمین کرد که در هنگام رخ دادن این رویداد (پر شدن حافظه)، نشست فعالی برای سرپرست اجرایی وجود داشته باشد، ارتباط باید از طریق سوابق ممیزی صورت گیرد.<br>وقتی که حافظه محلی برای ذخیره‌سازی داده ممیزی پر شد یا محصول به دلیل حافظه ناکافی با خطر از دست دادن داده مواجه شد، پیغام هشدار باید سرپرست را آگاه کند.<br>برای محصولات توزیع‌شده که امکان نمایش پیغام هشدار را پیاده‌سازی می‌کنند، باید توضیح داده شود که کدام مؤلفه این ویژگی را پشتیبانی می‌کند (وقتی که این ویژگی برای یک محصول انتخاب می‌گردد، نیاز نیست که تمامی مؤلفه‌های محصول آن را پشتیبانی کنند). در نهایت هر مؤلفه‌ای که این ویژگی را پشتیبانی می‌کند، باید یک پیغام هشدار را به‌وسیله خودش یا از طریق دیگر مؤلفه‌ها تولید کند.<br>اگر این الزام در سند هدف امنیتی آورده شود، آنگاه نویسنده سند هدف امنیتی باید شرایطی را که تحت آن داده به صورت غیرقابل مشاهده حذف می‌شود، ذکر کند. |

| شماره الزام | نام الزام |
|---|---|
| **۹۰** | **محل ذخیره‌سازی داده‌های ممیزی IPS** |
| محصول باید داده‌های IPS ذخیره شده را از حذف غیرمجاز محافظت نماید. | |
| **۹۱** | **محل ذخیره‌سازی داده‌های ممیزی ۲IPS** |

| شماره الزام | نام الزام |
|---|---|
| محصول باید قادر به [ جلوگیری] از تغییرات غیرمجاز در داده‌های IPS ذخیره شده، باشد.<br>**نکته کاربردی:**<br>رویدادهای قابل‌ممیزی IPS اضافه‌ای که نیاز باشد در «تولید داده ممیزی» در نظر گرفته شود، وجود ندارد. | |
| **۹۲** | **محل ذخیره‌سازی داده‌های ممیزی IPS ۷** |
| محصول در صورت پر شدن داده IPS، باید [انتخاب: «رویدادهای تولید شده توسط IPS را نادیده بگیرد»، «جلوگیری از ذخیره رویدادهای IPS»، «بر روی قدیمی‌ترین داده‌های IPS ذخیره شده دوباره‌نویسی کند».] | |

## ۶,۲ کلاس شناسایی و احراز هویت

| شماره الزام | نام الزام |
|---|---|
| **۹۳** | **الزامات پروتکل X509 (۱)/ تبادل داده کاربردی داخل محصول** |
| محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند:<br>• تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.<br>• مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.<br>• محصول مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل کند که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است<br>• محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 6960، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵، هیچ روش فسخ] تائید کند.<br>• محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند:<br>○ 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.<br>○ 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.<br><br>**نکته کاربردی:**<br>این الزام باید انتخاب گردد، در صورتی که محصول توزیع‌شده باشد و پروتکل (های) انتخاب شده در الزام FPT_ITT.1 از گواهی‌نامه‌های X.509 برای احراز هویت نظیر استفاده کنند. در این مورد، از آنجایی که الزامات اضافه‌ای در الزام FCO_CPC_EXT.1 در رابطه با فعال و غیر فعال‌سازی کانال ITT وجود دارد، استفاده از لیست فسخ اختیاری است. در صورتی که بررسی لیست فسخ پشتیبانی نمی‌شود، نویسنده سند هدف امنیتی باید گزینه «هیچ روش فسخ» را انتخاب کند. به هر حال، در صورت پشتیبانی، نویسنده سند هدف امنیتی باید مشخص کند که از OCSP یا RCL استفاده می‌گردد.<br>محصول باید از حداقل طول مسیر برای دو گواهی‌نامه پشتیبانی کند. بدین معنی که محصول باید از یک سلسله مراتب گواهی‌نامه که حداقل از گواهی‌نامه ریشه خود-امضاء[۱] و گواهی‌نامه هویت محصول تشکیل شده باشد، پشتیبانی کند.<br>سند خلاصه مشخصات محصول باید مشخص کند که چه مواقعی بررسی وضعیت فسخ انجام می‌گیرد. انتظار می‌رود که وقتی از گواهی‌نامه در احراز هویت استفاده می‌گردد، وضعیت فسخ نیز بررسی گردد. بررسی وضعیت یک گواهی‌نامه X509 فقط وقتی که روی دستگاه بارگذاری می‌شود، کافی نیست.<br>اگر محصول از هیچ‌کدام از موارد مطرح شده در قوانین extendedKeyUsage پشتیبانی نمی‌کند، این وضعیت باید در سند خلاصه مشخصات محصول شرح داده شود. |
| **۹۴ \| الزامات پروتکل X509 (۲) / تبادل داده کاربردی داخل محصول** |
| محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.<br><br>**نکته کاربردی:**<br>این الزام در مورد گواهی‌نامه‌هایی اعمال می‌شود که توسط محصول مورد ارزیابی بکار رفته و پردازش شده باشند. این الزام همچنین اضافه شدن گواهی‌نامه‌ها به لیست گواهی‌نامه‌های معتبر CA را محدود می‌کند. |

## ۶,۳ کلاس مدیریت امنیت

[۱] Self-signed root certificate

| شماره الزام | نام الزام |
|---|---|
| ۹۵ | **مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها** |
| محصول مورد ارزیابی باید توانایی فعال و غیرفعال کردن سرویس‌ها و توابع را به سرپرست امنیتی محدود کند.<br>**نکته کاربردی:**<br>این گزینه فقط زمانی باید انتخاب گردد که سرپرست امنیتی محصول توانایی آغاز و توقف سرویس‌ها را داشته باشد. در این مورد گزینه «آغاز و توقف سرویس‌ها» باید در «انتخاب» الزام FAU_GEN.1.1 انتخاب گردد.<br>همچنین عبارت «سرویس» نیز در نکته کاربردی دوم مطرح شده در الزام FAU_GEN.1.1 توضیح داده شده است. | |
| ۹۶ | **مدیریت داده‌های محصول ۱/ کلیدهای رمزنگاری** |
| محصول مورد ارزیابی باید توانایی مدیریت کردن کلیدهای رمزنگاری را به سرپرست امنیتی محدود کند.<br>**نکته کاربردی:**<br>این گزینه زمانی باید انتخاب گردد که سرپرست امنیتی امکان مدیریت کلیدهای رمزنگاری (برای مثال؛ اصلاح، حذف، تولید/واردکردن) را داشته باشد. این الزام مدیریت کلیدهای رمزنگاری را به سرپرست‌های امنیتی محدود می‌کند. عبارت "CryptoKeys" برای جداسازی این تکرار الزام FMT_MTD.1 از تکرار اجباری آن با نام FMT_MTD.1/CoreData است. | |

| شماره الزام | نام الزام |
|---|---|
| ۹۷ | **مدیریت رفتار توابع امنیتی IPS ۱** |
| محصول باید توانایی [تغییر رفتار] توابع [جمع‌آوری داده IPS، آنالیز کردن، واکنش] را به [ سرپرست مجاز IPS] محدود کند. | |
| ۹۸ | **مدیریت داده‌های محصول IPS ۱** |
| محصول باید قادر به محدود کردن [ انتخاب: تغییر پیش‌فرض، پرس‌وجو، ویرایش، حذف، پاک کردن، [اختصاص: عملیات دیگر]] و [اختصاص: لیستی از داده‌های IPS ] به [ اختصاص: سرپرست IPS، تحلیل‌گر IPS و دیگر نقش‌های مشخص‌شده در الزام «نقش امنیتی ۳»] باشد.<br><br>**نکته کاربردی:** | |

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

### ۶,۴ کلاس حفاظت از محصول مورد ارزیابی

| شماره الزام | نام الزام |
|---|---|
| ۹۹ | **انتقال داده امنیتی در داخل محصول ۱** |
| محصول باید از آشکارسازی داده توابع امنیتی محصول حفاظت کند و دست‌کاری/اصلاح در داده را وقتی که بین قسمت‌های مختلف محصول از طریق [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS ] مخابره می‌شود، تشخیص دهد.<br>**نکته کاربردی:**<br>این الزام فقط برای محصولات توزیع‌شده قابل اعمال است و اطمینان پیدا می‌کند که تمام ارتباطات میان مؤلفه‌های محصول از طریق یک کانال ارتباطی رمزگذاری شده، حفاظت می‌گیرد. داده‌ای که از طریق این کانال ارتباطی مورد اعتماد عبور داده می‌شود، به‌وسیله پروتکل انتخاب شده در عبارت «انتخاب» این الزام، رمزگذاری می‌گردد. نویسنده هدف امنیتی باید کانال‌ها و پروتکل‌های مورد استفاده توسط هر کدام از مؤلفه‌های یک ارتباط را مشخص کند.<br>این کانال ممکن است به عنوان کانال ثبت‌نام (داخل فرآیند ثبت‌نام در الزام FCO_CPC_EXT.1.2، توضیح داده شده است) استفاده گردد. | |
| ۱۰۰ | **مسیر امن ۱/ پیوند زدن** |
| محصول مورد ارزیابی باید مسیر ارتباطی میان خود و یک مؤلفه پیوندی[۱] که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم کند و [انتخاب: نقطه پایانی توابع امنیتی محصول، هر دو مورد (مؤلفه پیوندی و نقطه پایانی توابع امنیتی محصول)] را به صورت مطمئن شناسایی کرده و داده‌های تبادلی را در برابر تغییر [انتخاب: و افشاء، هیچ مورد دیگری] محافظت کند. | |
| ۱۰۱ | **مسیر امن ۲/ پیوند زدن** |
| محصول مورد ارزیابی باید به [انتخاب: توابع امنیتی محصول، مؤلفه پیوندی] اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند. | |
| ۱۰۲ | **مسیر امن ۳/ پیوند زدن** |

[۱] Joining

محصول مورد ارزیابی باید برای پیوند مؤلفه‌ها به توابع امنیتی تحت شرایط/قیدهای محیط عملیاتی تعریف شده که در راهنمای عملیاتی مورد اشاره قرار گرفته است، استفاده از کانال امن را الزامی کند.

**نکته کاربردی:**

این الزام (FTP_TRP.1/Join)، یکی از انواع کانال را که در اولین «انتخاب» در الزام FCO_CPC_EXT.1.2 بیان شده است، پیاده‌سازی می‌کند. عبارت «مؤلفه پیوندی» در الزام «مسیر امن ۱/پیوند زدن» در واقع یک موجودیت IT است که تلاش می‌کند از طریق فرآیند ثبت‌نام، به محصول توزیع‌شده بپیوندد.

هدف از الزام این است که برای مؤلفه‌ها امکان ارتباط با یک شیوه امن در زمان تشکیل توابع امنیتی فراهم گردد.

دومین «انتخاب» در الزام «مسیر امن ۱/پیوند زدن» در واقع بیان می‌کند که در برخی موارد، کانال ممکن است محرمانگی (حفاظت از آشکارسازی داده) را فراهم نکند؛ بنابراین، نویسنده هدف امنیتی باید در خلاصه مشخصات محصول بیان کند که در این مورد آیا محصول محرمانگی را روی محیط الزام می‌کند (از طریق «شرایط/قیدهای محیط عملیاتی تعریف شده» در همین الزام) یا اینکه داده تبادل شده نیاز به محرمانگی ندارد.

توجه شود که وقتی از FTP_TRP.1/Join برای کانال ثبت‌نام استفاده شود، سپس این کانال نمی‌تواند به عنوان یک کانال عادی ارتباطات میان مؤلفه‌ای مورد استفاده قرار گیرد. باید از FPT_ITT.1 یا FTP_ITC.1 استفاده شود.

### ۶,۵ کلاس ارتباطات

| شماره الزام | نام الزام |
|---|---|
| ۱۰۳ | **تعریف کانال ثبت‌نام مؤلفه ۱** |
| محصول باید سرپرست امنیتی را ملزم کند که قبل از اتفاق افتادن ارتباط میان هر جفت مؤلفه از محصول، برای آن‌ها یک ارتباط فعال کند. | |
| ۱۰۴ | **تعریف کانال ثبت‌نام مؤلفه ۲** |
| محصول باید یک فرآیند ثبت‌نام را پیاده‌سازی کند که در آن مؤلفه‌ها یک کانال ارتباطات را منتشر و استفاده کنند که این کانال حداقل برای داده توابع امنیتی محصول از [انتخاب:<br>• یک کانال که الزامات کانال امن را مطابق [انتخاب: FTP_ITC.1، FPT_ITT.1 ] رعایت کند.<br>• یک کانال که الزامات کانال ثبت‌نام امن را مطابق FTP_TRP.1/Join رعایت کند.<br>• هیچ کانالی] استفاده کند. | |
| ۱۰۵ | **تعریف کانال ثبت‌نام مؤلفه ۳** |
| محصول باید یک سرپرست امنیتی را فعال کند که بتواند کانال ارتباطات میان هر جفت مؤلفه از محصول را غیرفعال کند. | |

**نکته کاربردی:**
این الزام (FCO_CPC_EXT.1) فقط وقتی که محصول توزیع‌شده باشد و در نتیجه چند مؤلفه داشته باشد که نیاز به ارتباط از طریق کانال داخلی داشته باشند، قابل اعمال است.
انتخاب کانال در الزام «تعریف کانال ثبت‌نام مؤلفه ۲» اساساً یک انتخاب است بین اینکه از یک کانال امن معمولی که معادل است با الف) کانالی که برای ارتباط با موجودیت‌های خارجی (FTP_ITC.1) یا مؤلفه‌های محصول (FPT_ITT.1) استفاده می‌شود، یا ب) کانالی که برای ثبت‌نام بکار می‌رود (FTP_TRP.1/Join)، استفاده شود. در صورتی که محصول به دلیل امکان اقدامات پیکربندی قابل انجام توسط سرپرست محصول، نیاز به کانال ثبت‌نام نداشته باشد، آنگاه گزینه «هیچ کانالی» برای انتخاب الزام «تعریف کانال ثبت‌نام مؤلفه ۲» برگزیده می‌شود.
اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه سند خلاصه مشخصات محصول باید تکرارهایی از الزام را که برای مشخص کردن استفاده محصول لازم است، تشریح کند. در صورتی که FTP_TRP.1/Join انتخاب گردد، سند خلاصه مشخصات محصول (در صورت امکان با کمک سند راهنمای عملیاتی) باید جزییات کانال و سازوکارهایی را که استفاده می‌کند تشریح کند.
اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه در سند هدف امنیتی باید کانال ثبت‌نام به عنوان یکی از تکرارهای الزام FPT_ITT.1 یا FTP_ITC.1 با یک نام مشخص (مثال؛ FPT_ITT.1/Join)، در قالب نکته کاربردی به الزام «تعریف کانال ثبت‌نام مؤلفه ۱» اضافه و اجرا گردد.

## ۶,۶ الزامات محافظت از هدف ارزیابی

| شماره الزام | نام الزام |
|---|---|
| ۱۰۶ | **حفظ وضعیت امن در زمان شکست ۱** |
| محصول قادر است وضعیت امن را برای واسطهای درون‌خط وقتی که انواع شکست زیر روی می‌دهد حفظ کند:[اختصاص: لیست از انواع شکست توابع محصول] | |

## ۶,۷ الزامات تخصیص منابع

| شماره الزام | نام الزام |
|---|---|
| ۱۰۷ | **تخصیص منابع ۱** |
| محصول باید حداکثر سهمیه را برای منابع تخصیص دهد:[اختصاص: منابعی که از نظارت بر روی ترافیک شبکه پشتیبانی کنند] که [موجودیت‌های فعال] می‌توانند هم‌زمان استفاده کنند.<br>**نکته کاربردی:**<br>هدف این الزام حصول اطمینان از این است که محصول طوری توسعه داده نشده باشد که جریان داده روی واسطهای حس‌گر از مقداری که محصول می‌تواند بررسی کند، سرریز کند. اگر جریان (حجم/سرعت) داده که باید مورد بررسی قرار گیرد، از سهم تعیین شده سرریز کند، محصول باید یک اخطار در رابطه با این سرریز تولید کند. | |

### ۶,۸ کلاس دیواره آتش (FFW)

| شماره الزام | نام الزام |
|---|---|
| ۱۰۸ | 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.<br><br>نکته کاربردی:<br>این الزام پروتکل‌های بسیار پیچیده را مشخص می‌کند 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 می‌کند، پروتکل FTP به هر دو اتصال کنترلی و اتصال داده نیاز دارد.<br>درحالی‌که پورت‌های شناخته‌شده‌ای 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.<br>در حالت غیرفعال، سرور FTP ممکن است از پورت تصادفی>۱۰۲۳ به جای پورت ۲۰ استفاده کند. 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 کنند (به طور مثال، یک قانون نمی‌تواند پیش‌بینی کند که چه پورت تصادفی توسط کلاینت یا سرور استفاده می‌گردد و ممکن است به نظر آید که قانون پیش‌فرض، جلوگیری از اتصال روی پورت‌های تصادفی باشد.)
توابع امنیتی هدف ارزیابی، می‌تواند قوانین دینامیکی ایجاد کند 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 می‌کند تا شرایطی را مشخص کند که برای پروتکل‌های مشخصی در داخل فایروال اجازه می‌دهد که ارتباطات مورد انتظار با پورت‌های پیش‌بینی نشده UDP/TCP به صورت صحیح برقرار گردد.
اگر نویسنده هدف امنیتی، پروتکل‌های بیشتری را در برگیرد، نویسنده باید RFC که رفتار پروتکل را مشخص می‌کند را معرفی کند؛ همانند FTP در دومین مورد بالا.

### ۶,۹ الزامات IPS: جلوگیری از نفوذ

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

| شماره الزام | نام الزام |
|---|---|
| ۱۰۹ | **نرمال‌سازی ترافیک ۱** |
| محصول باید قادر به نظارت بر بسته‌های محصور شده از طریق [انتخاب:GRE، IP-in-IP،IPv4-in-IPv6،MPLS،PPTP، [اختصاص: دیگر روش‌های محصورسازی]، هیچ روش دیگر] باشد. | |
| ۱۱۰ | **نرمال‌سازی ترافیک ۲** |
| محصول باید قادر به نرمال‌سازی برای بازترکیب بسته‌های تکه‌تکه شده برای نظارت و [انتخاب:<br>• برای داده جمع شده در واسطهای promiscuous: در صورتی که نتوان بازترکیب را انجام داد، تولید یک پیام هشدار. | |

[۱] rulset

| شماره الزام | نام الزام |
|---|---|
| • برای داده جمع شده در واسط‌های درون‌خط: بسته‌های تکه‌تکه شده را هدایت نکرده و یک هشدار تولید کرده که نمی‌توان بسته موجود را بازترکیب کند.] | |
| ۱۱۱ | **نرمال‌سازی ترافیک ۳** |
| محصول باید نرمال‌سازی TCP را برای جریان‌های ترافیک از طریق محصول در حالتی که محصول در مد درون‌خط مستقر شده داشته باشد و از هدایت [انتخاب: بسته‌های تکراری، بسته‌های تغییر داده شده، بسته‌های خارج از توالی،[انتخاب: [اختصاص:دیگر انواع بسته‌ای که نباید ارسال گردد]، هیچ بسته دیگری]] جلوگیری کند. | |

## ۷ پیوست دو: الزامات مبتنی بر انتخاب

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

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

| ردیف | الزام | رویدادهای ممیزی | اطلاعات ممیزی ثبت‌شده |
|---|---|---|---|
| ۱. | الزامات پروتکل DTLS Client | شکست در ایجاد یک نشست DTLS | دلایل شکست |
| ۲. | الزامات پروتکل DTLS Client/ احراز هویت | شکست در ایجاد یک نشست DTLS | دلایل شکست |
| | | تشخیص حملات تکرار | هویت منبع حمله تکرار (مثلاً؛ آدرس IP) |
| ۳. | الزامات پروتکل DTLS Server | شکست در ایجاد یک نشست DTLS | دلایل شکست |
| | | تشخیص حملات تکرار | هویت منبع حمله تکرار (مثلاً؛ آدرس IP) |

| ردیف | الزام | رویدادهای ممیزی | اطلاعات ممیزی ثبت‌شده |
|---|---|---|---|
| ۴. | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه | شکست در ایجاد یک نشست DTLS | دلایل شکست |
| | | تشخیص حملات تکرار | هویت منبع حمله تکرار (مثلاً؛ آدرس IP) |
| ۵. | الزامات پروتکل HTTPS | شکست در ایجاد یک نشست HTTPS | دلایل شکست |
| ۶. | 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) |
| ۷. | 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) |
| ۸. | الزامات پروتکل TLS Client/ احراز هویت | شکست در ایجاد یک نشست TLS | دلایل شکست |
| ۹. | الزامات پروتکل TLS Client/ احراز هویت دوطرفه | شکست در ایجاد یک نشست TLS | دلایل شکست |
| ۱۰. | الزامات پروتکل TLS Server/ احراز هویت | شکست در ایجاد یک نشست TLS | دلایل شکست |
| ۱۱. | الزامات پروتکل TLS Server/ احراز هویت دوطرفه | شکست در ایجاد یک نشست TLS | دلایل شکست |
| ۱۲. | الزامات پروتکل X509(۱) و (۲)/ ابطال | تلاش‌های ناموفق برای اعتبارسنجی یک گواهی‌نامه. | دلایل شکست |
| ۱۳. | الزامات پروتکل X509(۳) و (۴) | - | - |
| ۱۴. | الزامات پروتکل X509(۵) و (۶) | - | - |
| ۱۵. | خودآزمایی محصول مورد ارزیابی ۲ | شکست در خودآزمایی | دلایل شکست (شامل شناساننده گواهی‌نامه‌های نامعتبر) |
| ۱۶. | الزامات به‌روزرسانی امن ۴ و ۵ | شکست در به‌روزرسانی | دلایل شکست (شامل شناساننده گواهی‌نامه‌های نامعتبر) |

| ردیف | الزام | رویدادهای ممیزی | اطلاعات ممیزی ثبت‌شده |
|---|---|---|---|
| .۱۷ | مدیریت کارکرد در محصول ۱/ به روزرسانی خودکار | فعال‌سازی و غیر فعال‌سازی جستجوی خودکار به‌روزرسانی‌ها یا به روزرسانی‌های خودکار | - |
| .۱۸ | مدیریت کارکرد در محصول ۱/ توابع | اصلاح یا تغییر رفتار؛ مخابره داده ممیزی به موجودیت IT خارجی، کنترل داده ممیزی، قابلیت عملکردی ممیزی وقتی که فضای محلی ذخیره‌سازی ممیزی پر باشد. | - |

**نکته کاربردی:**

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

- وجود افزونه basicConstraints و تائید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تائید 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 کرد.

### ۷,۱ الزامات پروتکل DTLS Client

| شماره الزام | نام الزام |
|---|---|
| **۱۱۲** | **الزامات پروتکل DTLS Client (۱)** |
| محصول باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:<br>• [انتخاب:<br>o TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268<br>o TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268<br>o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 | |

- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289

• ].

**نکته کاربردی:**

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

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

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

| ۱۱۳ | **الزامات پروتکل DTLS Client (۲)** |
|---|---|

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

**نکته کاربردی:**

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

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

[۱] Identifier

[۲] Background

| ۱۱۴ | الزامات پروتکل DTLS Client (۳) |
|---|---|
| محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].<br>**نکته کاربردی:**<br>اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. | |

| ۱۱۵ | الزامات پروتکل DTLS Client (۴) |
|---|---|
| محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب:secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.<br><br>**نکته کاربردی:**<br>اگر در الزام «الزامات پروتکل DTLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل DTLS Client (۱)» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت «Supported Elliptic Curves Extension را ارائه نکند» باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است. | |

### ۷,۲ الزامات پروتکل DTLS Clint /احراز هویت

| شماره الزام | نام الزام |
|---|---|
| ۱۱۶ | **الزامات پروتکل DTLS Client/ احراز هویت ۱** |
| محصول باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:<br>• [انتخاب:<br>o TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268<br>o TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268<br>o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 | |

- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289

• ].

**نکته کاربردی:**

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

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

| ۱۱۷ | **الزامات پروتکل DTLS Client/ احراز هویت ۲** |
|---|---|

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

**نکته کاربردی:**

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

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

| ۱۱۸ | **الزامات پروتکل DTLS Client/ احراز هویت ۳** |
|---|---|

[۱] Identifier

[۲] Background

| |
|---|
| محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].<br>**نکته کاربردی:**<br>اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. |
| **۱۱۹ \| الزامات پروتکل DTLS Client/ احراز هویت ۴** |
| محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.<br><br>**نکته کاربردی:**<br>اگر در الزام «الزامات پروتکل DTLS Client/ احراز هویت ۱» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل DTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت «Supported Elliptic Curves Extension را ارائه نکند» باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است. |
| **۱۲۰ \| الزامات پروتکل DTLS Client/ احراز هویت ۵** |
| محصول باید احراز هویت دوطرفه را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی کند.<br>**نکته کاربردی:**<br>استفاده از گواهی‌نامه‌های X509v3 برای پروتکل DTLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که کلاینت باید برای احراز هویت دوطرفه DTLS، قادر باشد یک گواهی‌نامه به سرور DTLS ارائه کند. |
| **۱۲۱ \| الزامات پروتکل DTLS Client/ احراز هویت ۶** |
| محصول باید هنگامی که یک پیام حاوی MAC نامعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد].<br>**نکته کاربردی:** |

| |
|---|
| کد احراز هویت پیام (MAC) در واقع یک تابع هش کلید است که در الزام FCS_COP.1/KeyedHash شرح داده شده است. این کد در طی فاز دست‌تکانی DTLS مخابره می‌شود و برای حفاظت از جامعیت پیام‌های است که از طرف فرستنده در مبادله داده DTLS، دریافت می‌شود. اگر تائید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بی‌صدا دور انداخته شود. |

| ۱۲۲ | **الزامات پروتکل DTLS Client/ احراز هویت ۷** |
|---|---|

محصول باید پیام‌های تکرار/بازپخش[۱] شده برای موارد زیر را تشخیص و بی‌صدا دور بیندازد:

- رکوردهای DTLS که قبلاً دریافت شده است.
- رکوردهای DTLS که برای پنجره لغزنده، قدیمی محسوب می‌شود.

**نکته کاربردی:**

تشخیص بازپخش در بخش 4.1.2.6 از DTLS v1.2 (RFC 6347) و بخش 4.1.2.5 از DTLS v1.0 (RFC 4347) تشریح شده است. برای هر رکورد دریافتی، دریافت‌کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف شده باشد و قبلاً توسط رکوردهای دریافت شده، استفاده نشده باشد؛ یعنی پیام تکرار نباشد.

## ۷,۳ الزامات پروتکل DTLS Server

| شماره الزام | نام الزام |
|---|---|
| ۱۲۳ | **الزامات پروتکل DTLS Server (۱)** |

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

- [انتخاب:
  - TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
  - TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268
  - TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492

[۱] Replayed

- TLS_ECDHE_RSA_WITH_AES_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289
- ].

**نکته کاربردی:**

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

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

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

| ۱۲۴ | **الزامات پروتکل DTLS Server (۲)** |
|---|---|

محصول باید برای کلاینت‌های دارای درخواست [هیچ موردی]، ارتباطات را ایجاد نکند.

**نکته کاربردی:**

این پروفایل حفاظتی، محصول را ملزم به رد کردن درخواست DTLS v1.0 نمی‌کند. در نسخه آتی این پروفایل حفاظتی درخواست‌های DTLS v1.0 باید توسط تمامی محصولات، رد شود.

| ۱۲۵ | **الزامات پروتکل DTLS Server (۳)** |
|---|---|

محصول نباید در صورت شکست خوردن اعتبارسنجی DTLS Client، تلاش دست‌تکانی ارتباط را پیش ببرد.

**نکته کاربردی:**

فرآیند اعتبارسنجی کردن DTLS Client در بخش 4.2.1 از DTLS v1.2 (RFC 6347) و DTLS v1.0 (RFC 4347) تشریح شده است. محصول DTLS Client را قبل از ارسال پیام ServerHello توسط توابع امنیتی محصول و در طی برقراری ارتباط (دست‌تکانی)، اعتبارسنجی می‌کند. سرور بعد از دریافت ClientHello، یک پیغام HelloVerifyRequest را از کوکی به کلاینت ارسال می‌کند. کوکی درواقع یک پیام امضاء شده با استفاده از توابع هش معرفی شده در الزام FCS_COP.1/KeyedHash است. کلاینت دوباره یک پیغام ClientHello را به همراه کوکی امضاء شده ارسال می‌کند، سرور در صورت تائید کردن کوکی ارسالی کلاینت، مطمئن می‌شود که کلاینت از آدرس IP جعلی استفاده نکرده است.

| ۱۲۶ | **الزامات پروتکل DTLS Server (۴)** |
|---|---|

محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] اجرا کند؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری، تولید کند؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت] تولید کند].

**نکته کاربردی:**

| |
|---|
| اگر سند هدف امنیتی در الزام «الزامات پروتکل DTLS Server (۱)» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_SMF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط DTLS ملزم می‌کند که از لحاظ امنیتی قوی باشد. |

| ۱۲۷ | **الزامات پروتکل DTLS Server (۵)** |
|---|---|
| محصول باید هنگامی که یک پیام حاوی MAC نامعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد]. |
| **نکته کاربردی:** |
| کد احراز هویت پیام (MAC) در واقع یک تابع هش کلید است که در الزام FCS_COP.1/KeyedHash شرح داده شده است. این کد در طی فاز دست‌تکانی DTLS مخابره می‌شود و برای حفاظت از جامعیت پیام‌های است که از طرف فرستنده در مبادله داده DTLS، دریافت می‌شود. اگر تائید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بی‌صدا دور انداخته شود. |

| ۱۲۸ | **الزامات پروتکل DTLS Server (۶)** |
|---|---|
| محصول باید پیام‌های تکرار/بازپخش شده برای موارد زیر را تشخیص و بی‌صدا دور بیندازد:<br>• رکوردهای DTLS که قبلاً دریافت شده است.<br>• رکوردهای DTLS که برای پنجره لغزنده، قدیمی محسوب می‌شود. |
| **نکته کاربردی:** |
| تشخیص بازپخش در بخش 4.1.2.6 از DTLS v1.2 (RFC 6347) و بخش 4.1.2.5 از DTLS v1.0 (RFC 4347) تشریح شده است. برای هر رکورد دریافتی، دریافت‌کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف شده باشد و قبلاً توسط رکوردهای دریافت شده، استفاده نشده باشد؛ یعنی پیام تکرار نباشد.<br>عبارت «بی‌صدا دور بیندازد» یعنی محصول بدون هیچ‌گونه پاسخی بسته را دور بیندازد. |

### ۷,۴ الزامات پروتکل DTLS Server /احراز هویت دوطرفه

| شماره الزام | نام الزام |
|---|---|
| ۱۲۹ | **الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱** |
| محصول باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:<br>• [انتخاب:<br>○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 | |

- TLS_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289<br>○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289<br>○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289<br>○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289<br>○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289<br>• ].<br><br>**نکته کاربردی:**<br>مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند.<br>نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 6347، الزامی است.<br>در نسخه‌های آتی این پروفایل حفاظتی، DTLS v1.2 برای همه محصولات الزامی می‌گردد. |
| **۱۳۰ الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۲** |
| محصول باید برای کلاینت‌های دارای درخواست [هیچ موردی]، ارتباطات را ایجاد نکند.<br>**نکته کاربردی:**<br>این پروفایل حفاظتی، محصول را ملزم به رد کردن درخواست DTLS v1.0 نمی‌کند. در نسخه آتی این پروفایل حفاظتی درخواست‌های DTLS v1.0 باید توسط تمامی محصولات، رد شود. |
| **۱۳۱ الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۳** |
| محصول نباید در صورت شکست خوردن اعتبارسنجی DTLS Client، تلاش دست‌تکانی ارتباط را پیش ببرد.<br>**نکته کاربردی:**<br>فرآیند اعتبارسنجی کردن DTLS Client در بخش 4.2.1 از DTLS v1.2 (RFC 6347) و DTLS v1.0 (RFC 4347) تشریح شده است. محصول DTLS Client را قبل از ارسال پیام ServerHello توسط توابع امنیتی محصول و در طی برقراری ارتباط (دست‌تکانی)، اعتبارسنجی می‌کند. سرور بعد از دریافت ClientHello، یک پیغام HelloVerifyRequest را از کوکی به کلاینت ارسال می‌کند. کوکی درواقع یک پیام امضاء شده با استفاده از توابع هش معرفی شده در الزام FCS_COP.1/KeyedHash است. کلاینت دوباره یک پیغام ClientHello را به همراه کوکی امضاء شده ارسال می‌کند، سرور در صورت تائید کردن کوکی ارسالی کلاینت، مطمئن می‌شود که کلاینت از آدرس IP جعلی استفاده نکرده است. |

| ۱۳۲ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۴ |
|---|---|
| محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] اجرا کند؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری، تولید کند؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت] تولید کند].<br><br>**نکته کاربردی:**<br>اگر سند هدف امنیتی در الزام «الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_MOF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط DTLS ملزم می‌کند که از لحاظ امنیتی قوی باشد. | |
| ۱۳۳ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۵ |
| محصول باید هنگامی که یک پیام حاوی MAC نامعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد].<br>**نکته کاربردی:**<br>کد احراز هویت پیام (MAC) در واقع یک تابع هش کلید است که در الزام FCS_COP.1/KeyedHash شرح داده شده است. این کد در طی فاز دست‌تکانی DTLS مخابره می‌شود و برای حفاظت از جامعیت پیام‌های است که از طرف فرستنده در مبادله داده DTLS، دریافت می‌شود. اگر تائید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بی‌صدا دور انداخته شود. | |
| ۱۳۴ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۶ |
| محصول باید پیام‌های تکرار/بازپخش شده برای موارد زیر را تشخیص و بی‌صدا دور بیندازد:<br>• رکوردهای DTLS که قبلاً دریافت شده است.<br>• رکوردهای DTLS که برای پنجره لغزنده، قدیمی محسوب می‌شود.<br>**نکته کاربردی:**<br>تشخیص بازپخش در بخش 4.1.2.6 از DTLS v1.2 (RFC 6347) و بخش 4.1.2.5 از DTLS v1.0 (RFC 4347) تشریح شده است. برای هر رکورد دریافتی، دریافت‌کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف شده باشد و قبلاً توسط رکوردهای دریافت شده، استفاده نشده باشد؛ یعنی پیام تکرار نباشد.<br>عبارت «بی‌صدا دور بیندازد» یعنی محصول بدون هیچ‌گونه پاسخی بسته را دور بیندازد. | |
| ۱۳۵ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۷ |
| محصول باید احراز هویت دوطرفه کلاینت‌های DTLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی کند. | |

| ۱۳۶ | الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۸ |
|---|---|
| محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].<br>**نکته کاربردی:**<br>استفاده از گواهی‌نامه‌های X509v3 برای پروتکل DTLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که گواهی‌نامه‌های سمت کلاینت باید برای احراز هویت دوطرفه DTLS پشتیبانی گردند.<br>اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. | |
| ۱۳۷ | **الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۹** |
| محصول در صورت مطابقت نداشتن؛ نام متمایز[۱] یا نام دیگر فاعل[۲] موجود در گواهی‌نامه، با آنچه از شناساننده[۳] کلاینت انتظار بوده است، نباید کانال امن را برقرار سازد.<br>**نکته کاربردی:**<br>شناساننده کلاینت ممکن است در فیلد subject یا افزونه نام دیگر فاعل مربوط به یک گواهی‌نامه باشد. شناساننده مورد انتظار باید پیکربندی گردد. این شناساننده ممکن است با نام دامنه، آدرس IP، یا آدرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود. | |

## ۷,۵ الزامات پروتکل HTTPS

| شماره الزام | نام الزام |
|---|---|
| ۱۳۸ | **الزامات پروتکل HTTPS (۱)** |
| محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند.<br>**نکته کاربردی:**<br>نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان عناصری را به این مؤلفه افزود یا اطلاعاتی را به خلاصه مشخصات محصول اضافه کرد. | |

[۱] Distinquish Name (DN)

[۲] Subject Alternative Name (SAN)

[۳] Identifier

| ۱۳۹ | الزامات پروتکل HTTPS (۲) |
|---|---|
| محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند. | |
| ۱۴۰ | الزامات پروتکل HTTPS (۳) |
| درصورتی‌که گواهی‌نامه همتا ارائه شده باشد و نامعتبر باشد، محصول مورد ارزیابی باید [انتخاب: اتصال را برقرار نکند، برای برقراری اتصال درخواست مجوز کند، هیچ اقدام دیگری انجام ندهد].<br><br>**نکته کاربردی:**<br>اگر در الزام FTP_ITC.1 یا FTP_TRP.1/Admin پروتکل HTTPS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی‌نامه بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT.1 پروتکل HTTPS انتخاب گردد، آنگاه اعتبار گواهی‌نامه بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. | |

## ۷,۶ الزامات پروتکل SSH Client

| شماره الزام | نام الزام |
|---|---|
| ۱۴۱ | الزامات پروتکل SSH Client (۱) |
| محصول باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251، 4252، 4253، 4254، 5647، 5656، 6187، 6668، هیچ RFC دیگری] پیاده‌سازی کند.<br><br>**نکته کاربردی:**<br>نویسنده سند هدف امنیتی انتخاب می‌کند که با کدام‌یک از RFC ها مطابقت وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً؛ الگوریتم‌های رمزنگاری معتبر). RFC 4253 الگوریتم‌های رمزنگاری مشخص را که "REQUIRED" (موردنیاز) هستند، تعیین می‌کند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شود، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. مشخص کردن اینکه کدام‌یک از الگوریتم‌هایی که به صورت "REQUIRED" می‌باشند، لیست شده ولی پیاده‌سازی نشده است، در حوزه فعالیت ارزیابی این الزام قرار نمی‌گیرد. | |

| ۱۴۲ | الزامات پروتکل SSH Client (۲) |
|---|---|
| محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه در RFC 4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر گذرواژه، هیچ روش دیگری]. | |
| ۱۴۳ | الزامات پروتکل SSH Client (۳) |
| همان‌طور که در RFC 4253 توضیح داده‌شده است، محصول باید اطمینان حاصل کند که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH، کنار گذاشته شوند.<br><br>**نکته کاربردی:**<br>RFC 4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول معقولی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازهٔ بستهٔ قابل پذیرش پر شود تا به این وسیله «طول معقول» برای محصول تعریف شود. | |
| ۱۴۴ | الزامات پروتکل SSH Client (۴) |
| محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [انتخاب: AES128-CBC، AES-256-CBC، AES128-CTR، AES256-CTR، AEAD_AES_128_GCM، AEAD_AES_256_GCM] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.<br>**نکته کاربردی:**<br>RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند. | |
| ۱۴۵ | الزامات پروتکل SSH Client (۵) |
| محصول باید اطمینان حاصل کند که پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد کند.<br>**نکته کاربردی:**<br>اگر x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521 انتخاب گردند، آنگاه لیستی از مراجع گواهی امن باید در الزام FCS_SSHC_EXT.1.9 انتخاب شود و الزامات FCS_X509_EXT قابل اعمال خواهند بود. | |

| ۱۴۶ | الزامات پروتکل SSH Client (۶) |
|---|---|
| محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512 ] و [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، هیچ الگوریتم MAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.<br>**نکته کاربردی:**<br>RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند. RFC 6668 استفاده از sha2 را در SSH مشخص می‌کند. | |
| ۱۴۷ | الزامات پروتکل SSH Client (۷) |
| محصول باید اطمینان حاصل کند 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. | |
| ۱۴۸ | الزامات پروتکل SSH Client (۸) |
| محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه؛ طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد.<br>**نکته کاربردی:**<br>این الزام حد آستانه‌هایی را برای، حداکثر زمانی که یک کلیدهای نشست می‌تواند استفاده گردد و حداکثر مقدار داده‌ای که می‌تواند با یک کلیدهای نشست، انتقال یابد. هر دو حد آستانه باید پیاده‌سازی گردد و یک مجددسازی کلید نیز وقتی هر کدام از دو مورد مذکور سر برسد، باید بکار گرفته شود. برای محاسبه حداکثر داده انتقالی، داده‌هایی که به محصول وارد و از محصول خارج می‌شوند باید محاسبه گردد. مجددسازی کلید باید روی تمام کلیدهای نشست (رمزنگاری، حفاظت از جامعیت) برای ترافیک ورودی و خروجی اعمال گردد.<br>محصول همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکر شده در این الزام را پیاده‌سازی کند.<br>سند راهنمای محصول، باید نحوه پیکربندی این مقادیر و نحوه سر رسیدن آن‌ها و همچنین چگونگی امکان تعریف مقادیر کمتر از حد آستانه را تشریح کند. | |
| ۱۴۹ | الزامات پروتکل SSH Client (۹) |

| |
|---|
| محصول باید اطمینان حاصل کند که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن یا [انتخاب: فهرستی از مراجع صدور گواهی مطمئن، هیچ روش دیگری] (تشریح شده در RFC 4251 بخش ۴,۱) همراه می‌کند، استفاده می‌کند.<br>**نکته کاربردی:**<br>تنها در صورتی می‌توان گزینه «فهرستی از مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521 در «الزامات پروتکل SSH Client (۵)» انتخاب‌شده باشد. |

## ۷,۷ الزامات پروتکل SSH Server

| شماره الزام | نام الزام |
|---|---|
| ۱۵۰ | **الزامات پروتکل SSH Server (۱)** |
| محصول باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251، 4252، 4253، 4254، 5647، 5656، 6187، 6668، هیچ RFC دیگری] پیاده‌سازی کند.<br><br>**نکته کاربردی:**<br>نویسنده سند هدف امنیتی انتخاب می‌کند که با کدام‌یک از RFC ها مطابقت وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً؛ الگوریتم‌های رمزنگاری معتبر). 4253 RFC الگوریتم‌های رمزنگاری مشخص را که "REQUIRED" (موردنیاز) هستند، تعیین می‌کند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شود، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. مشخص کردن اینکه کدام‌یک از الگوریتم‌هایی که به صورت "REQUIRED" می‌باشند، لیست شده ولی پیاده‌سازی نشده است، در حوزه فعالیت ارزیابی این الزام قرار نمی‌گیرد. | |
| ۱۵۱ | **الزامات پروتکل SSH Server (۲)** |
| محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC 4252 توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر گذرواژه. | |
| ۱۵۲ | **الزامات پروتکل SSH Server (۳)** |

| |
|---|
| همان‌طور که در RFC 4253 توضیح داده‌شده است، محصول باید اطمینان حاصل کند که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH، کنار گذاشته شوند.<br><br>**نکته کاربردی:**<br>RFC 4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول معقولی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول معقول» برای محصول تعریف شود. |
| **۱۵۳ \| الزامات پروتکل SSH Server (۴)** |
| محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [انتخاب: AES128-CBC، AES-256-CBC، AES128-CTR، AES256-CTR، AEAD_AES_128_GCM، AEAD_AES_256_GCM] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.<br>**نکته کاربردی:**<br>RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند. |
| **۱۵۴ \| الزامات پروتکل SSH Server (۵)** |
| محصول باید اطمینان حاصل کند که پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد کند.<br>**نکته کاربردی:**<br>اگر x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521 انتخاب گردند، آنگاه الزامات FCS_X509_EXT قابل اعمال خواهند بود. |
| **۱۵۵ \| الزامات پروتکل SSH Server (۶)** |
| محصول باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512 ] و [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، هیچ الگوریتم MAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند. |

| |
|---|
| **نکته کاربردی:**<br>RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند. RFC 6668 استفاده از sha2 را در SSH مشخص می‌کند. |

| ۱۵۶ | **الزامات پروتکل SSH Server (۷)** |
|---|---|
| محصول باید اطمینان حاصل کند 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. | |

| ۱۵۷ | **الزامات پروتکل SSH Server (۸)** |
|---|---|
| محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه؛ طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد. | |

| |
|---|
| **نکته کاربردی:**<br>این الزام حد آستانه‌هایی را برای، حداکثر زمانی که یک کلیدهای نشست می‌تواند استفاده گردد و حداکثر مقدار داده‌ای که می‌تواند با یک کلیدهای نشست، انتقال یابد. هر دو حد آستانه باید پیاده‌سازی گردد و یک مجددسازی کلید نیز وقتی هر کدام از دو مورد مذکور سر برسد، باید بکار گرفته شود. برای محاسبه حداکثر داده انتقالی، داده‌هایی که به محصول وارد و از محصول خارج می‌شوند باید محاسبه گردد. مجددسازی کلید باید روی تمام کلیدهای نشست (رمزنگاری، حفاظت از جامعیت) برای ترافیک ورودی و خروجی اعمال گردد.<br>محصول همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکر شده در این الزام را پیاده‌سازی کند.<br>سند راهنمای محصول، باید نحوه پیکربندی این مقادیر و نحوه سر رسیدن آن‌ها و همچنین چگونگی امکان تعریف مقادیر کمتر از حد آستانه را تشریح کند. |

### ۷,۸ الزامات پروتکل TLS Client

| شماره الزام | نام الزام |
|---|---|
| ۱۵۸ | **الزامات پروتکل TLS Client (۱)** |

محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند.
همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:
[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

].

**نکته کاربردی:**

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

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است.

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

| ۱۵۹ | **الزامات پروتکل TLS Client (۲)** |
|---|---|

محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید کند.

**نکته کاربردی:**

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

| |
|---|
| روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده کند. |
| **۱۶۰** **الزامات پروتکل TLS Client (۳)** |
| محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].<br>**نکته کاربردی:**<br>اگر در الزام FTP_TRP.1/Admin یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT پروتکل TLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. |
| **۱۶۱** **الزامات پروتکل TLS Client (۴)** |
| محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب:secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.<br><br>**نکته کاربردی:**<br>اگر در الزام «الزامات پروتکل TLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل TLS Client (۱)» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت «Supported Elliptic Curves Extension را ارائه نکند» باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است. |

## ۷,۹ الزامات پروتکل TLS Client/ احراز هویت

| شماره الزام | نام الزام |
|---|---|
| ۱۶۲ | **الزامات پروتکل TLS Client/ احراز هویت ۱** |

محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند.
همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:
[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289

- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

].

**نکته کاربردی:**

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

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است.

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

| ۱۶۳ | **الزامات پروتکل TLS Client/ احراز هویت ۲** |
|---|---|

محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید کند.

**نکته کاربردی:**

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

| |
|---|
| برای قسمت Subject Alternative Name را منتشر می‌کند. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند.<br>روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده کند. |
| **۱۶۴** **الزامات پروتکل TLS Client/ احراز هویت ۳** |
| محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].<br>**نکته کاربردی:**<br>اگر در الزام FTP_TRP.1/Admin یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT پروتکل TLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. |
| **۱۶۵** **الزامات پروتکل TLS Client/ احراز هویت ۴** |
| محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.<br><br>**نکته کاربردی:**<br>اگر در الزام «الزامات پروتکل TLS Client/ احراز هویت ۱» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل TLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت «Supported Elliptic Curves Extension را ارائه نکند» باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است. |
| **۱۶۶** **الزامات پروتکل TLS Client/ احراز هویت ۵** |
| محصول باید احراز هویت دوطرفه را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی کند. |

**نکته کاربردی:**
استفاده از گواهی‌نامه‌های X509v3 برای پروتکل TLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که کلاینت باید برای احراز هویت دوطرفه TLS، قادر باشد یک گواهی‌نامه به سرور TLS ارائه کند.

## ۷,۱۰ الزامات پروتکل TLS Server

| شماره الزام | نام الزام |
|---|---|
| ۱۶۷ | **الزامات پروتکل TLS Server (۱)** |

محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند.
همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:
[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با RFC 5246

- TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

].

**نکته کاربردی:**

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

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است.

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

| ۱۶۸ | **الزامات پروتکل TLS Server (۲)** |
|---|---|

| |
|---|
| محصول باید برای کلاینت‌های دارای درخواست SSL 2.0، SSL 3.0، TLS 1.0 [انتخاب: TLS 1.1، TLS 1.2، هیچ موردی]، ارتباطات را ایجاد نکند.<br>**نکته کاربردی:**<br>تمامی نسخه‌های SSL و TLS v1.0 رد می‌شوند. هر نسخه‌ای از TLS که در الزام «الزامات پروتکل TLS Server (۱)» انتخاب نگردد، باید در الزام آورده شود. |

| ۱۶۹ | **الزامات پروتکل TLS Server (۳)** |
|---|---|

| |
|---|
| محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] اجرا کند؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری، تولید کند؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت] تولید کند].<br><br>**نکته کاربردی:**<br>اگر سند هدف امنیتی در الزام «الزامات پروتکل TLS Server (۱)» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_SMF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط TLS ملزم می‌کند که از لحاظ امنیتی قوی باشد. |

### ۷,۱۱ الزامات پروتکل TLS Server/ احراز هویت دوطرفه

| شماره الزام | نام الزام |
|---|---|
| ۱۷۰ | **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱** |

| |
|---|
| محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند.<br>همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند:<br>[انتخاب:<br>o TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268<br>o TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268<br>o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 |

- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

| |
|---|
| ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289<br>○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289<br>○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289<br>]. |
| **نکته کاربردی:**<br>مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند.<br>نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است.<br>در نسخه‌های آتی این پروفایل حفاظتی، TLS v1.2 برای همه محصولات الزامی می‌گردد. |
| **۱۷۱** \| **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۲** |
| محصول باید برای کلاینت‌های دارای درخواست SSL 2.0، SSL 3.0، TLS 1.0 [انتخاب: TLS 1.1، TLS 1.2، هیچ موردی]، ارتباطات را ایجاد نکند.<br>**نکته کاربردی:**<br>تمامی نسخه‌های SSL و TLS v1.0 رد می‌شوند. هر نسخه‌ای از TLS که در الزام «الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱» انتخاب نگردد، باید در الزام آورده شود. |
| **۱۷۲** \| **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳** |
| محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] اجرا کند؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1 ] و هیچ منحنی دیگری، تولید کند؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت] تولید کند].<br>**نکته کاربردی:**<br>اگر سند هدف امنیتی در الزام «الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_SMF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط TLS ملزم می‌کند که از لحاظ امنیتی قوی باشد. |
| **۱۷۳** \| **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۴** |

| |
|---|
| محصول باید احراز هویت دوطرفه کلاینت‌های TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی کند. |
| **۱۷۴** \| **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۵** |
| محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور نامعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].<br>**نکته کاربردی:**<br>استفاده از گواهی‌نامه‌های X509v3 برای پروتکل TLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که گواهی‌نامه‌های سمت کلاینت باید برای احراز هویت دوطرفه TLS پشتیبانی گردند.<br>اگر در الزام FTP_TRP یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.<br>اگر در الزام FTP_ITT پروتکل TLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود. |
| **۱۷۵** \| **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۶** |
| محصول در صورت مطابقت نداشتن؛ نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده[۱] کلاینت انتظار بوده است، نباید کانال امن را برقرار سازد.<br>**نکته کاربردی:**<br>شناساننده کلاینت ممکن است در فیلد subject یا افزونه نام دیگر فاعل مربوط به یک گواهی‌نامه باشد. شناساننده مورد انتظار باید پیکربندی گردد. این شناساننده ممکن است با نام دامنه، آدرس IP، یا آدرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود. |

## ۷,۱۲ الزامات شناسایی و احراز هویت

| شماره الزام | نام الزام |
|---|---|
| ۱۷۶ | **الزامات پروتکل X509 (۱) / ابطال** |
| محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند:<br>• تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. | |

[۱] Identifier

- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.
- محصول مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل کند که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است
- محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 6960، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵، هیچ روش فسخ] تائید کند.
- محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند:
  - گواهی‌نامه‌های مورداستفاده برای تائید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف « Code Signing» (id-kp 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.

| ۱۷۷ | **الزامات پروتکل X509 (۲)/ ابطال** |
|---|---|

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

**نکته کاربردی:**

الزام «الزامات پروتکل X509 (۱)/ ابطال» قوانین برای تائید گواهی‌نامه‌ها را فهرست می‌کند. نویسنده سند هدف امنیتی باید مشخص کند که تائید ابطال بر اساس OCSP یا CRLs انجام می‌گیرد. پروتکل‌های مسیر/کانال امن ممکن است استفاده از گواهی‌نامه‌ها را الزامی کنند؛ در این صورت، قوانین ExtendedKeyUsage باید بررسی و تائید شده باشند. اگر محصول قابلیت عملکردی که از انواع گواهی‌نامه‌های فهرست شده در قوانین ExtendedKeyUsage استفاده می‌کند را پشتیبانی نمی‌کند، این وضعیت باید در سند خلاصه مشخصات محصول شرح داده شود.

| |
|---|
| محصول باید از حداقل طول مسیر برای دو گواهی‌نامه پشتیبانی کند. بدین معنی که محصول باید از یک سلسله مراتب گواهی‌نامه که حداقل از گواهی‌نامه ریشه خود-امضاء و گواهی‌نامه هویت محصول تشکیل شده باشد، پشتیبانی کند.<br>انتظار می‌رود که تائید گواهی‌ها تا یک گواهی‌نامه CA ریشه مورد اعتماد در داخل یک منبع ریشه که به‌وسیله پلتفرم مدیریت می‌شود، انجام گیرد.<br>سند خلاصه مشخصات محصول باید مشخص کند که چه مواقعی بررسی وضعیت فسخ انجام می‌گیرد. انتظار می‌رود که وقتی از گواهی‌نامه در احراز هویت استفاده می‌گردد، وضعیت فسخ نیز بررسی گردد. بررسی وضعیت یک گواهی‌نامه X509 فقط وقتی که روی دستگاه بارگذاری می‌شود، کافی نیست.<br>بررسی و تائید کردن وضعیت ابطال گواهی‌نامه‌های X509، حین روشن شدن و خودآزمایی‌ها ضروری نیست.<br>الزام «الزامات پروتکل X509 (۲)/ ابطال» 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.<br>نویسنده سند هدف امنیتی در تمامی موارد به جزء؛ وقتی فقط SSH در FTP_ITC.1 یا FPT_ITT.1 انتخاب گردد و احراز هویت به ssh-rsa، ssh-sha2-nistp256، ssh-sha2-nistp384 یا/و ssh-sha2-nistp521 محدود شده باشد، باید الزامات «الزامات پروتکل X509 (۱) و (۲)/ ابطال» را وارد کند. به علاوه، وقتی که در FPT_TUD_EXT یا FPT_TST_EXT استفاده از گواهی X509 انتخاب گردد، الزامات «الزامات پروتکل X509 (۱) و (۲)/ ابطال» باید آورده شود. |

| ۱۷۸ | **الزامات پروتکل X509 (۳)** |
|---|---|
| محصول مورد ارزیابی باید جهت پشتیبانی احراز هویت برای [انتخاب: IPsec, DTLS, TLS, HTTPS, SSH] و [انتخاب: امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم، امضای کد برای تائید یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند. | |

| ۱۷۹ | **الزامات پروتکل X509 (۴)** |
|---|---|
| زمانی که محصول مورد ارزیابی نمی‌تواند اتصال مورد نیاز برای تائید 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:**

در الزام «الزامات پروتکل X509 (۳)»، انتخاب نویسنده سند هدف امنیتی شامل IPsec، TLS، یا HTTPS می‌شود در صورتی که این پروتکل‌های در الزامات FTP_ITC.1.1 یا FPT_ITT.1 گنجانده شده باشند. اگر احراز هویتی غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و/یا ecdsa-sha2-nistp521، در الزام «الزامات پروتکل SSH Client (۵)» بیان شده باشد یا

| |
|---|
| گواهی‌نامه‌های آن برای به‌روزرسانی‌های امن نرم‌افزار سیستم (FPT_TUD_EXT.2) و تائید جامعیت (FPT_TST_EXT.2) استفاده شده باشد، آنگاه الزام «الزامات پروتکل X509 (۳)» باید پروتکل SSH را نیز شامل گردد.<br>معمولاً برای بررسی وضعیت فسخ یک گواهی‌نامه باید اتصالی را برقرار کرد. این اتصال هم برای دانلود کردن یک CRL و هم برای جستجو با استفاده از OCSP لازم است. با استفاده از «انتخاب» در این الزام، می‌توان تعیین کرد که اگر برقراری این اتصال ممکن نباشد، باید چه اقدامی را انجام داد. اگر محصول مورد ارزیابی بر اساس تمام قوانین مورداشاره در الزامات «الزامات پروتکل X509 (۱) و (۲)» به این نتیجه برسد که گواهی‌نامه معتبر است، می‌تواند آن را بپذیرد. اگر هر یک از این قوانین نشان‌دهنده عدم تائید گواهی‌نامه باشند، محصول مورد ارزیابی نباید آن را بپذیرد. اگر نویسنده هدف امنیتی انتخاب اول را انجام دهد و به سرپرست محصول قدرت تصمیم‌گیری بدهد، باید تابع مربوطه از FMT_SMF.1 را نیز انتخاب کند. این انتخاب باید با الزامات FCS_IPSEC_EXT.1.14، FCS_TLSC_EXT.1.3 و FCS_TLSC_EXT.2.3 سازگار باشد.<br>در صورتی که محصول توزیع‌شده باشد و الزام FIA_X509_EXT.1/ITT برای آن انتخاب شده باشد، بررسی وضعیت فسخ گواهی، اختیاری است. |
| **۱۸۰ الزامات پروتکل X509 (۵)** |
| محصول مورد ارزیابی باید مطابق با آنچه در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند اطلاعات؛ کلید عمومی و [انتخاب: اطلاعات مخصوص به دستگاه[۱]، Common Name، Orgsnization، Organization Unit، Country] را در درخواست فراهم کند.<br><br>**نکته کاربردی:**<br>کلید عمومی در واقع بخش عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آنچه در FCS_CKM.1 شرح داده‌شده است، توسط محصول مورد ارزیابی تولید می‌شود. |
| **۱۸۱ الزامات پروتکل X509 (۶)** |
| محصول مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند. |

## ۷,۱۳ الزامات خودآزمایی محصول مورد ارزیابی

[۱] Device-specific information

| شماره الزام | نام الزام |
|---|---|
| ۱۸۲ | **خودآزمایی محصول مورد ارزیابی ۲** |
| اگر برای آزمون‌های خودآزمایی از یک گواهی‌نامه استفاده شود و آن گواهی‌نامه نامعتبر اعلام‌شده باشد، محصول باید در آزمون خودآزمایی ناموفق باشد.<br><br>**نکته کاربردی:**<br>گواهی‌نامه‌ها را می‌توان به‌صورت اختیاری برای آزمون‌های خودآزمایی استفاده کرد (FPT_TST_EXT.1.1). اگر برای آزمون‌های خودآزمایی از گواهی‌نامه‌ها استفاده شود، سند هدف امنیتی باید شامل این مورد باشد. اگر در «الزامات پروتکل X509 (۳)» مقدار «امضای کد برای تائید یکپارچگی» انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی ۲» باشد. اعتبار به‌وسیله مسیر گواهی‌نامه، تاریخ انقضاء و وضعیت ابطال مطابق با FIA_X509_EXT.1/Rev تعیین می‌گردد. | |
| ۱۸۳ | **الزامات به‌روزرسانی امن ۴** |
| محصول درصورتی‌که گواهی‌نامه امضای کد یک به‌روزرسانی نامعتبر باشد، نباید آن را نصب کند. | |
| ۱۸۴ | **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 کند، گواهی را بپذیرد، گواهی را نپذیرد].<br><br>**نکته کاربردی:**<br>گواهی‌نامه‌ها را می‌توان به‌صورت اختیاری برای امضای کدها در به‌روزرسانی‌های نرم‌افزار سیستم استفاده کرد (FPT_TUD_EXT.1.3). اگر در «الزامات پروتکل X509 (۳)» مقدار «امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم» انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی ۲» باشد. در صورتی که فقط از هش‌های انتشار یافته برای به‌روزرسانی‌های امن پشتیبانی گردد، گواهی X509 قابل اعمال نیست.<br>اعتبار به‌وسیله مسیر گواهی‌نامه، تاریخ انقضاء و وضعیت ابطال مطابق با تمامی FIA_X509_EXT.1/Rev 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. | |

## ۷,۱۴ الزامات به‌روزرسانی امن

| شماره الزام | نام الزام |
|---|---|
| ۱۸۵ | **مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار** |
| محصول باید قابلیت [انتخاب: فعال کردن و غیرفعال کردن] توابع [انتخاب: جستجو برای به‌روزرسانی‌های خودکار، به‌روزرسانی خودکار] را به سرپرست امنیتی محصول محدود کند.<br><br>**نکته کاربردی:**<br>این الزام تنها زمانی قابل پیاده‌سازی است که محصول امکان پشتیبانی از جستجو برای به‌روزرسانی‌های خودکار و/یا به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال کردن این قابلیت‌ها را بدهد. فعال کردن و غیرفعال کردن جستجو برای به‌روزرسانی‌های خودکار و/یا به‌روزرسانی خودکار به سرپرست‌های امنیتی محصول محدود شده است. گزینه «به‌روزرسانی خودکار» ممکن است فقط وقتی انتخاب شود که از امضاء دیجیتال برای تائید به‌روزرسانی امن استفاده گردد. | |
| ۱۸۶ | **مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع** |
| محصول باید قابلیت [انتخاب: تعیین رفتار[۱]، تغییر/اصلاح رفتار[۲]] مربوط به توابع [انتخاب: مخابره داده ممیزی به موجودیت IT خارجی، کنترل داده ممیزی، قابلیت عملکردی ممیزی در صورت پر بودن فضای محلی ذخیره‌سازی] را به سرپرست امنیتی محصول محدود کند.<br><br>**نکته کاربردی:**<br>این الزام در صورتی انتخاب می‌گردد که یک یا چند مورد از سناریوهای زیر اعمال شوند:<br>• اگر پروتکل انتقال برای ارسال داده ممیزی به موجودیت IT خارجی که در الزام FAU_STG_EXT.1.1 تعریف شده است، قابل پیکربندی باشد و «ارسال داده ممیزی به موجودیت IT خارجی» انتخاب شده باشد.<br>• اگر کنترل داده ممیزی قابل پیکربندی باشد، «کنترل داده ممیزی» باید انتخاب گردد. عبارت «کنترل داده ممیزی» به گزینه‌های مختلفی برای انتخاب و اختصاص در الزامات FAU_STG_EXT.1.2، FAU_STG_EXT.1.3 و FAU_STG_EXT.2/LocSpace اشاره دارد. | |

[۱] Determine the behaviour

[۲] Modify the behaviour

- اگر رفتار قابلیت عملکردی ممیزی وقتی که فضای محلی ذخیره‌سازی ممیزی پر است، قابل پیکربندی باشد. عبارت «قابلیت عملکرد ممیزی در صورت پر بودن فضای محلی ذخیره‌سازی» باید انتخاب گردد.

# ۸ تعاریف

## ۸,۱ تعریف حملات

| نام | توضیحات |
|---|---|
| DoS | حمله DoS (Denial of Service) |
| Flooding | جاری ساختن سیل عظیمی از ترافیک روی یک زیرشبکه IP یا علیه یک آدرس IP خاص |
| IP Impossible Packet (Land) | بسته‌های IP که آدرس مبدأ و مقصد آن‌ها یکسان است (Land Attack) |
| IP options Bad Option List | دیتاگرام IP که لیست گزینه‌های IP در سرآیند آن ناقص یا دستکاری‌شده هستند. |
| IP options Record Packet Route | دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۷ می‌شود (Record Packet Route) |
| IP options Timestamp | دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۴ می‌شود (Timestamp) |
| IP options Security | دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۲ می‌شود (Security) |
| IP options Loose Source Route | دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۳ می‌شود (Loose Source Route) |
| IP options Strict Source Route | دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۲ می‌شود (Strict Source Route) |
| IP Overlapping Fragments (Teardrop, Bonk) | دو تکه داده موجود در یک دیتاگرام IP واحد دارای آفست‌هایی دال بر موقعیت مشترک آن‌ها در دیتاگرام هستند. این امر می‌تواند بدین معنی باشد که تکه الف به طور کامل یا ناقص توسط تکه ب بازنویسی شده است. |

| نام | توضیحات |
|---|---|
| ICMP fragments (Ping of Death, Nuke) | فیلد پروتکل سربرگ IP دیتاگرام IP روی ۱ تنظیم می‌شود (ICMP)، بیت تکه آخر[۱] تنظیم می‌گردد و (آفست IP * ۸) + (طول داده IP) باید بزرگ‌تر از ۶۵۵۳۵ باشد. آفست ارائه‌دهنده موقعیت ابتدایی این تکه در بسته اولیه است و در واحدهای ۸ بایتی قرار دارد) به علاوه بقیه بسته، بزرگ‌تر از حداکثر اندازه یک بسته IP است. |
| ICMP flooding (Smurf, ping flood) | آدرس IP مقصد در بسته عبارت است از آدرس پخش[۲] زیرشبکه مقصد، به گونه‌ای که تمام ماشین‌های روی این زیرشبکه به پخش پاسخ دهند. |
| Scanning (IP protocols, TCP ports, UDP ports) | تلاش برای تعیین اینکه آیا خدمات گوش دادن روی برخی شماره‌های پروتکل IP، پورت‌های TCP یا پورت‌های UDP خاص موجود هستند یا خیر. برای این کار، مجموعه‌ای از داده‌ها ارسال می‌شوند تا یک پاسخ مورد انتظار تولید گردد. |
| TCP FIN only flags | بسته‌های TCP FIN بی‌هویت[۳]، به یک پورت دارای دسترسی ویژه فرستاده می‌شوند (شماره پورت‌های کمتر از ۱۰۲۴) |
| TCP flood (SYN flood) | ارسال تعداد بسیار زیادی بسته TCP با پرچم SYN تنظیم‌شده به منظور فزونی گرفتن از محدودیت تعداد نشست‌های TCP نیمه‌باز. |
| TCP NULL flags | یک بسته TCP که هیچ‌یک از پرچم‌های SYN، FIN، ACK یا RST آن تنظیم نشده است به یک میزبان خاص فرستاده می‌شود. |
| TCP SYN+FIN flags | بسته TCP که پرچم‌های SYN و FIN آن تنظیم شده است. |
| UDP Bomb attack | طول UDP تعیین‌شده کمتر از طول IP تعیین‌شده است. این نوع بسته تغییرشکل‌یافته با یک حمله DoS همراه می‌شود. |
| UDP Chargen DoS attack | بسته UDP دارای پورت مبدأ ۷ و پورت مقصد ۱۹ است. |

[۱] Last Fragment bit
[۲] Broadcast
[۳] Orphaned TCP FIN packet

## ۸,۲ تعریف عبارات و مخففها

| نام | توضیحات |
|---|---|
| ناهنجاری / ناهنجار (در مورد ترافیک شبکه) | ترافیکی که در دسته ترافیک‌های عادی تعریف‌شده نمی‌گنجد و بنابراین، غیرمنتظره و غیر نوعی است. ترافیک ناهنجار الزاماً خطرناک نیست و ضرورتاً شبکه پایش‌شده را تهدید نمی‌کند. |
| ترافیک عادی[۱] (در مورد ترافیک شبکه) | تعریف می‌کند که کدام ترافیک‌های شبکه پایش‌شده، مورد انتظار یا عادی هستند. تمام ترافیک‌های عادی (ترافیک مبنا) الزاماً امن نیستند و عادی بودن ترافیک به این معنی نیست که تهدیدی برای شبکه پایش‌شده به شمار نمی‌آید. به عنوان مثال، ترافیک عادی می‌تواند با لیست آدرس‌های IP بد انطباق داشته باشد یا مطابق با امضای تهدیدات شناخته‌شده باشد. |
| مُد جریان درونی[۲] | به‌کارگیری محصول (یا مؤلفه‌های آن) به گونه‌ای که ترافیک شبکه پایش‌شده الزاماً از محصول بگذرد و بدین ترتیب، محصول امکان مسدود کردن آن را داشته باشد. |
| IPS | سیستم پیشگیری از نفوذ[۳] |
| خط‌مشی IPS (خط‌مشی پیشگیری از نفوذ) | تمام مجموعه قوانینی که برای تحلیل ترافیک، مسدود کردن ترافیک، تشخیص امضا و/یا تشخیص ناهنجاری استفاده می‌شوند. بسیاری از خط‌مشی‌های IPS را می‌توان تعریف و روی محصول ذخیره کرد؛ اما این خط‌مشی‌ها بدون پیاده‌سازی (فعال‌سازی) روی یک یا چند واسط IPS اثری نخواهند داشت. |

[۱] Baseline
[۲] Inline mode
[۳] Intrusion Prevention System

| نام | توضیحات |
|---|---|
| نرمال‌سازی (در مورد ترافیک شبکه) | فیلتر کردن ترافیک شبکه به گونه‌ای که تنها بسته‌ها یا تکه‌های مفید اجازه رسیدن به مقصد را داشته باشند. نرمال‌سازی تنها در صورتی توسط محصول قابل انجام است که محصول در مد جریان درونی به کار گرفته شده باشد. در فرایند نرمال‌سازی ممکن است بسته‌های تکراری، تکه‌هایی که نمی‌توان سر هم کرد، بسته‌های نامعتبر و بسته‌های دارای خارج از توالی، کنار گذاشته و فیلتر شوند. |
| پروفایلینگ (در مورد ترافیک شبکه) | مانند تعریف ترافیک عادی. |
| مُد بی‌قاعده[۱] | حالتی از یک واسط IP که در آن واسط مذکور به ترافیک شبکه گوش می‌دهد (آن‌ها را جمع‌آوری و بازرسی می‌کند). ممکن است منظور از یک واسط بی‌قاعده، واسطی باشد که فقط به ترافیک گوش می‌دهد و هرگز آن را منتشر نمی‌کند، یا واسطی که مثلاً در مد جریان درونی قرار دارد و جریان ورودی و خروجی ترافیک در آن برقرار است. |
| واسط حسگر | هر واسط محصول که خط‌مشی IPS در آن پیاده‌سازی شده است. |

# ۹ مراجع

- **Network Devices cPP V2.0 published by Network iTC**

[۱] Promiscuous mode