.

به نام خدا

پروفایل حفاظتی مسیریاب

نسخه ۲

مرداد ماه ۹۳

پیش‌گفتار

این سند توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است که معرفی کننده الزامات کارکرد امنیتی برای مسیریاب‌ها می‌باشد تا تولیدکنندگان مسیریاب‌ها[1] بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ نموده و همچنین سند هدف امنیتی آن را ارائه نمایند.

در بخش اول به معرفی این دسته از محصولات پرداخته شده است. سپس در بخشی تحت عنوان «مسائل امنیتی» تهدیدهایی که محصول با آنها روبرو است و فرضیاتی که در رابطه با امنیت محصول در نظر گرفته شده است و همچنین خط‌مشی‌های آن عنوان می‌شود.

سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدها، اجرای خط‌مشی‌ها و بکاربردن فرضیات مطرح می‌شود.

در بخش بعدی «الزامات کارکرد امنیتی» آورده شده است. براساس استاندارد معیار مشترک این قسمت از چندین کلاس تشکیل شده است که هریک از این کلاس‌ها حوزه خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای مسیریاب در این سند مطرح شده است عبارتند از:

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس حفاظت از داده‌های کاربری
- کلاس شناسایی و احراز هویت

---

1 Router

- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی
- کلاس دسترسی به هدف ارزیابی
- کلاس تخصیص منابع
- هر کلاس مجموعه‌ای از خانواده و هر خانواده مجموعه‌ای از مؤلفه و هر مؤلفه مجموعه‌ای از عناصر می‌باشد. با استفاده از «الزامات کارکرد امنیتی» در واقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌شود.
- 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.

لازم به ذکر است که مسیریاب‌ها علاوه بر «مسائل امنیتی»، «الزامات کارکرد امنیتی» و «الزامات تضمین» ذکر شده در این سند، تمام موارد «پروفایل حفاظتی تجهیزات شبکه »را نیز در بر می‌گیرند.

فهرست

۱ هدف از ارائه سند

در راستای ارزیابی امنیتی محصولات مبتنی بر «استاندارد ارزیابی معیار مشترک» لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده کردن الزامات ارائه شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود.

۲ معرفی اصطلاحات

- **هدف ارزیابی (TOE)**

به سیستم مورد ارزیابی براساس «استاندارد ارزیابی معیار مشترک»، هدف ارزیابی گفته می‌شود.

- **غیر هدف ارزیابی (Non-TOE[1])**

سخت‌افزار، نرم‌افزار و میان افزاری که هدف ارزیابی جهت اجرا به آن‌ها نیز نیاز دارد.

- **محیط عملیاتی (Operational Environment)**

محیطی که هدف ارزیابی در آن عمل می‌کند.

1 Non-Target Of Evaluation

- **پروفایل حفاظتی (PP[1])**

بیانیه‌ای از الزامات امنیتی برای یک نوع از هدف ارزیابی، که الزامات امنیتی را به صورت کلی بیان می‌دارد.

- **هدف امنیتی (ST[2])**

بیانیه‌ای از الزامات امنیتی برای هدف ارزیابی خاصی، که الزامات امنیتی را به صورت جزئی‌تر بیان می‌دارد. این بیانیه معمولاً توسط سازنده هدف ارزیابی نوشته می‌شود.

- **مسائل امنیتی (Security Problem)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «مشکل امنیتی» وجود دارد که به طور رسمی ماهیت و حوزه امنیت در نظر گرفته شده توسط هدف ارزیابی را تعریف می‌کند.

این بیانیه شامل موارد زیر است:

- «تهدیدهایی» که توسط هدف ارزیابی و محیط عملیاتی‌اش مقابله می‌شود.
- «خط‌مشی امنیت سازمانی» که توسط هدف ارزیابی و محیط عملیاتی‌اش اجرا می‌شود.
- «فرضیاتی» که برای محیط عملیاتی هدف ارزیابی تائید می‌شوند.

1 Protection Profile

2 Security Target

- **عامل تهدید (Threat Agent)**

موجودیت‌هایی که می‌توانند بر روی دارایی‌ها اقدام تهاجمی انجام دهند.

- **خط‌مشی امنیتی سازمانی (OSP[1])**

مجموعه‌ای از قوانین، که توصیف کننده رفتار امنیتی خاصی است که توسط «توابع امنیتی هدف ارزیابی» اجرا می‌شوند؛ این مجموعه قوانین به صورت یک مجموعه از «الزام‌های کارکرد امنیتی» قابل بیان است.

- **اهداف امنیتی (Security Objective)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «اهداف امنیتی» وجود دارد که برای مقابله با تهدیدها معرفی شده و/یا برای برآورده کردن خط‌مشی‌های امنیت سازمان و یا فرضیات معرفی شده در بخش «مسائل امنیتی»، در نظر گرفته شده است.

- **الزام امنیتی (Security Requirement)**

الزاماتی که به زبان استاندارد بیان می‌شود تا در حاصل شدن اهداف ارزیابی، برای هدف ارزیابی کمک نمایند.

- **الزام کارکرد امنیتی (SFR[2])**

بیان کننده کارکردهای امنیتی هدف ارزیابی در قالب کلاس می‌باشد. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام کارکرد امنیتی» وجود دارد.

---

1 Organizational Security Policy

2 Security Functional Requirement

- **الزامات تضمین امنیتی (SAR[1])**

این دسته از الزامات اطمینان می‌دهند که الزامات کارکرد امنیتی توسط هدف ارزیابی برآورده می‌شوند. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام تضمین امنیتی» وجود دارد.

- **بسته (Package)**

نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی می‌باشد. به عنوان مثال EAL3.

- **سطح تضمین ارزیابی (EAL[2])**

مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است و نشان دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» می‌باشد.

- **توابع امنیتی هدف ارزیابی (TSFs[3])**

آن بخش از هدف ارزیابی که برای اجرای صحیح «الزامات کارکرد امنیتی» باید به آن تکیه نمود، به عنوان «توابع امنیتی هدف ارزیابی» نام برده می‌شود. «توابع امنیتی هدف ارزیابی» شامل تمام سخت‌افزار، نرم‌افزار و میان‌افزارهای هدف ارزیابی است که مستقیم و غیرمستقیم برای اجرا شدن امنیت باید به آنها تکیه نمود.

- **داده توابع امنیتی هدف ارزیابی (TSF data)**

1 Security Assurance Requirement

2 Evaluation Assurance Level

3 TOE Security Functions

داده‌هایی برای عملیات هدف ارزیابی هستند که اجرای الزامات کارکرد امنیتی وابسته به آنها می‌باشد. این داده‌ها اطلاعات استفاده شده توسط توابع امنیتی هدف ارزیابی هستند.

- **داده کاربری (User data)**

داده‌های کاربری هستند که عملکرد توابع امنیتی هدف ارزیابی را تحت تاثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به کار برده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری می‌باشد.

- **کلاس (Class)**

مجموعه‌ای از خانواده‌های «استاندارد ارزیابی معیار مشترک» که روی یک موضوع متمرکز، اشتراک دارند.

- **خانواده (Family)**

مجموعه‌ای از عناصر که بر روی یک هدف اشتراک دارند اما در دقت و میزان تاکید، تفاوت دارند.

- **عنصر (Component)[۱]**

کوچکترین مجموعه از مؤلفه‌های قابل انتخاب، که الزامات ممکن است براساس آن‌ها باشد.

- **مؤلفه (Element)[۲]**

بیانی از نیاز امنیتی که غیر قابل تجزیه است.

---

۱ در استاندارد ملی ایران ISO 15408 **منتشر شده توسط سازمان ملی استاندارد،** Component **مؤلفه ترجمه شده است.**

۲ در استاندارد ملی ایران ISO 15408 **منتشر شده توسط سازمان ملی استاندارد،** Element **عنصر ترجمه شده است.**

- **اختصاص (Assignment)**

مشخص کردن پارامترهای معرفی شده در یک مؤلفه (از استاندارد معیار مشترک) یا الزام می‌باشد.

- **انتخاب (Selection)**

انتخاب کردن یک یا بیش از یک آیتم در لیستی که در مؤلفه یا الزام وجود دارد.

- **سرپرست (Administrator)**

موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی هدف ارزیابی بر عهده دارد و معمولا دارای بالاترین سطح مجوز است.

- **موجودیت فعال (Subject)**

موجودیت فعال، موجودیتی در سیستم مورد ارزیابی (هدف ارزیابی) است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره. به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی هدف ارزیابی است.

- **موجودیت غیرفعال (Object)**

موجودیت غیرفعال، موجودیتی در سیستم مورد ارزیابی (هدف ارزیابی) می‌باشد که شامل اطلاعات است یا اطلاعات را دریافت می‌کند و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره. به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله کننده، که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

- **راز (Secret)**

اطلاعاتی که باید تنها به کاربران مجاز و/یا توابع امنیتی هدف ارزیابی شناسانده شود، تا یک «خط‌مشی کارکرد امنیتی » اجرا شود.

- **مشخصه امنیتی(Security Attribute)**

کاربران، موجودیت‌های فعال، اطلاعات، موجودیت‌های غیرفعال، نشست‌ها و منابع تحت کنترل قوانین «الزامات کارکرد امنیتی» ممکن است دارای اطلاعات خاصی باشند که جهت کارکرد صحیح هدف ارزیابی، مورد استفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند هم‌چون نام فایل که ممکن است برای معرفی منابع منحصر به فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به طور خاص برای اجرا شدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به طور کلی «مشخصه امنیتی» نامیده می‌شود.

- **خط‌مشی کارکرد امنیتی(SFP[1])**

رفتار امنیتی که توسط «کارکرد امنیتی هدف ارزیابی» اجرا می‌شود تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شوند، این مجموعه قوانین «خط مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که هدف ارزیابی باید اجرا کند، تعریف کند. هر کدام از خط‌مشی‌ها باید حوزه کنترلی‌اش را توسط موجودیت‌های فعال، موجودیت‌های غیرفعال، منابع یا اطلاعات و عملکردهایی که بکار برده است، مشخص کند. تمام این خط‌مشی‌ها توسط «توابع امنیتی هدف ارزیابی» پیاده‌سازی می‌شوند.

1 Security Functionality Policy

- **خط‌مشی کارکرد امنیتی کنترل دسترسی (Access Control SFP)**

چندین خط‌مشی کارکرد امنیتی وجود دارد که برای حفاظت از داده‌ها بکار برده می‌شوند، همچون «خط‌مشی کنترل دسترسی» و «خط مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، TSF status data و عملکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

این مشخصه‌های امنیتی در مجموعه قوانینی استفاده می‌شوند که حاکم بر عملیاتی است که موجودیت‌های فعال ممکن است بر روی موجودیت‌های غیرفعال اجرا نمایند.

- **خط‌مشی کنترل جریان اطلاعات (Information Flow Control SFP)**

«خط‌مشی جریان اطلاعات» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی‌شان و مجموعه قوانین حاکم بر عملیات که توسط موجودیت فعال بر روی اطلاعات صورت می‌گیرد، پیاده‌سازی می‌شوند.

۳ معرفی استاندارد ۱۵۴۰۸

استاندارد ISO/IEC 15408 که به عنوان استاندارد ارزیابی معیار مشترک[1]نیز شناخته می‌شود با هدف تعیین مبنایی جهت ارزیابی ویژگی‌های امنیتی محصولات فناوری اطلاعات و سیستم‌ها تدوین گردیده است. با ایجاد چنین مبنایی با معیار مشترک، نتایج ارزیابی امنیتی فناوری اطلاعات برای تعداد بیشتری از مخاطبین حائز اهمیت خواهد بود.

استاندارد ISO/IEC 15408 در برگیرنده مؤلفه‌های کارکرد امنیتی بوده که مبنایی برای ارزیابی الزامات کارکرد امنیتی موجود در پروفایل حفاظتی یا سند هدف امنیتی است. این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[2]یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده کردن اهداف امنیتی که در پروفایل حفاظتی یا سند هدف امنیتی تعیین شده، می‌باشد.

استاندارد ISO/IEC 15408 در سه بخش ارائه شده است :

بخش اول: مقدمه و مدل عمومی (اصطلاحات و واژگان)

بخش دوم: الزامات کارکرد امنیتی [3]

بخش سوم: الزامات تضمین امنیتی[4]

---

1 Common Criteria (CC)

2 Target Of Evaluation (TOE)

3 Security Functional Requirement (SFR)

4 Security Assurance Requirement (SAR)

۴ معرفی مسیریاب

این پروفایل حفاظتی حداقل الزامات امنیتی برای هدف ارزیابی در این سند که مسیریاب می‌باشد را مشخص نموده است.

۴,۱ نوع محصول

محصول مسیریابی که مطابق این پروفایل حفاظتی است، از قابلیت‌های مانیتور کردن، مسیریابی و دستکاری ترافیک شبکه پشتیبانی می‌کند تا انتقال بسته‌ها به مقصد مناسب یا بین شبکه‌ها را تسهیل کند.

پروفایل حفاظتی مسیریاب جهت ارائه دادن یک هدف و معیار برای به‌کارگیری دستگاه‌های مسیریاب ایجاد شده است. این پروفایل حفاظتی معرفی کننده عملکرد امنیتی می‌باشد و تضمین می‌کند که مجموعه حداقلی از الزامات امنیتی در این پروفایل نشان داده شده است این پروفایل حفاظتی قابل اجرا به محصولات است صرف نظر از اینکه آنها خارج یا داخل شبکه هستند. لازم به ذکر است که این پروفایل تنها الزامات امنیتی را در نظر می‌گیرد و در برگیرنده ملاحظات خاص طراحی محصول نمی‌باشد. پروفایل حفاظتی مسیریاب تنها آن معیارهایی را آدرس‌دهی می‌کند که باید در زمان روبه‌رو شدن با یک مسیریاب اختصاصی در نظر گرفته شود. این پروفایل نباید قابلیت‌های اضافی که ممکن است به مسیریاب اضافه شود را درنظر بگیرد (مانند رمزنگاری داده شبکه کاربری نقطه به نقطه و نظارت و دستکاری ترافیک دقیق) که در واقع مسیریاب را به نوع دیگری از دستگاه‌ها هم‌چون نقطه پایانی شبکه اختصاصی مجازی(VPN) یا دیوار آتش تغییر می‌دهد. این نوع از دستگاه‌ها باید تحت پروفایل حفاظتی مناسب خودشان پوشش داده شوند.

۴,۲ تعریف هدف ارزیابی

مسیریاب دستگاهی است که بسته‌های داده را در امتداد شبکه ارسال می‌کند. مسیریاب حداقل به دو شبکه متصل می‌شود. (معمولاً دو شبکه LAN وWAN یا یک شبکه LAN و یک شبکه ISP). مسیریاب‌ها در دروازه‌ها قرار می‌گیرند، موقعیتی که دو یا بیش از دو شبکه به هم متصل می‌شوند. مسیریاب‌ها از سرایند و جداول پیشرو[1] جهت تعیین بهترین مسیر برای ارسال بسته‌ها استفاده می‌نمایند، هم‌چنین مسیریاب‌ها از پروتکل‌هایی هم‌چون ICMP[2] جهت ارتباط با یکدیگر استفاده می‌نمایند و بهترین مسیر بین هر دو میزبان را پیکربندی می‌نمایند. یک مسیریاب می‌تواند به گونه‌ای پیکربندی شود تا از چندین پروتکل شبکه پشتیبانی نماید و پروتکل‌های بر روی یک دستگاه واحد را مسیریابی نمایند.

1 Forwarding tables

2 Internet Control Message Protocol

۵ تعریف مسائل امنیتی

۵,۱ فرضیات

A.TYPE	توضیحات
A.NO_GENERAL_PURPOSE	فرض شده است که قابلیت محاسباتی همه منظوره (به طور مثال، کامپایلر یا برنامه‌های کاربردی) به غیر از سرویس‌های لازم برای عملیات، سرپرستی و پشتیبانی از هدف ارزیابی در دسترس هدف ارزیابی نمی‌باشد.
A.PHYSICAL	امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌های مربوط به آن است و فرض می‌شود که امنیت فیزیکی توسط محیط فراهم می‌شود.
A.AVAILABILITY	منابع شبکه باید در دسترس قرار گیرند تا به کلاینت‌ها برای برآوردن الزامات ماموریت و انتقال اطلاعات اجازه دهند.

۵,۲ تهدیدها

T.TYPE	توضیحات
T.ADMIN_ERROR	سرپرست ممکن است به طور ناخواسته هدف ارزیابی را به صورت ناصحیح نصب و پیکربندی کند و سبب ناکارآمد شدن سازوکارهای امنیتی شود.
T.ADMIN_ROGUE	مقاصد سرپرست ممکن است مخرب باشند و منجر به خطر افتادن داده توابع امنیتی هدف ارزیابی و کاربری شوند.

T.RESIDUAL_DATA	یک کاربر یا پروسه ممکن است بواسطه تخصیص مجدد منابع هدف ارزیابی از یک کاربر یا پروسه به دیگری، سبب دسترسی غیرمجاز به هدف ارزیابی شود.
T.AUDIT_COMPROMISE	کاربر یا پروسه مخرب ممکن است رکوردهای ممیزی را مشاهده کند و سبب از دست رفتن یا تغییر یافتن رکوردهای ممیزی شود، یا از ثبت رکوردهای ممیزی در آینده جلوگیری کند، بنابراین مانع دیده شدن اقدامات کاربر شود.
T.CRYPTO_COMPROMISE	کاربر یا پروسه مخرب ممکن است سبب شود که کلید، داده یا کد اجرایی مرتبط با عملکرد رمزنگاری به صورت نامناسبی دسترسی داشته باشند (دیده شود، تغییر یابد یا حذف شود)، بنابراین سازوکارهای رمزنگاری و داده محافظت شده توسط این سازوکارها به خطر می‌افتد.
T.FLAWED_DESIGN	در مشخصات یا طراحی هدف ارزیابی ممکن است خطاهای عمدی یا غیرعمدی رخ دهد که منجر به نقص‌هایی شود که کاربر یا برنامه مخرب از آنها در راستای اهدافشان بهره برداری کند.
T.FLAWED_IMPLEMENTATION	در پیاده‌سازی طراحی هدف ارزیابی ممکن است خطاهای عمدی یا غیرعمدی رخ دهد که منجر به نقص‌هایی شود که کاربر یا برنامه مخرب از آنها در راستای اهدافشان بهره برداری کند.
T.MALICIOUS_TSF_COMPROMISE	یک کاربر یا پروسه مخرب ممکن است سبب دسترسی نامناسب (مشاهده شود، تغییر یابد یا حذف شود) کد اجرایی یا داده توابع امنیتی هدف ارزیابی شود.
T.MASQUERADE	یک کاربر، پروسه یا موجودیت IT خارجی ممکن است جهت به دست آوردن دستیابی به داده یا منابع هدف ارزیابی، به جای یک موجودیت مجاز جا زده شود.

T.POOR_TEST	عدم آزمون یا آزمون‌های ناکافی که نشان می‌دهد تمام عملکرد هدف ارزیابی به درستی عمل می‌کند، ممکن است سبب کشف نشدن رفتار نادرست هدف ارزیابی که سبب آسیب‌پذیری‌های امنیتی بالقوه می‌شود، شود.
T.RESOURCE_EXHAUSTION	یک پروسه یا کاربر مخرب ممکن است از طریق حمله «انکار اتلاف منابع سرویس» [1]از منابع سیستمی دیگران را بلوکه کند.
T.SPOOFING	یک کاربر، پروسه مخرب یا موجودیت IT خارجی ممکن است خودش را به عنوان هدف ارزیابی معرفی کند تا بتواند داده‌های شناسایی و احراز هویت را به دست آورد.
T.UNATTENDED_SESSION	یک کاربر ممکن است به یک نشست بی‌مراقب، دسترسی غیرمجازی داشته باشد.
T.REPLAY	یک کاربر ممکن است به هدف ارزیابی از طریق تکرار اطلاعات احراز هویت دسترسی نامناسبی به دست آورد یا ممکن است بواسطه تکرار کردن داده توابع امنیتی هدف ارزیابی یا مشخصه‌های امنیتی، سبب تنظیم نامناسب هدف ارزیابی شود.
T.UNIDENTIFIED_ACTIONS	ممکن است سرپرست در توجه و شناسایی نقض‌های امنیتی بالقوه دچار خطا شود که در نتیجه توانایی سرپرست برای شناسایی و اقدام علیه نقض‌های امنیتی

1 Resource exhaustion denial of service attack

	محدود می‌شود.
T.UNAUTHORIZED_ACCESS	ممکن است کاربر دسترسی به داده‌های کاربری داشته باشد که مطابق با خط-مشی امنیت هدف ارزیابی نسبت به آن‌ها غیر مجاز باشد.
T.UNAUTHORIZED_PEER	یک موجودیت IT غیر مجاز ممکن است تلاش کند تا یک ارتباط امنیتی با هدف ارزیابی را ایجاد کند.
T.UNKNOWN_STATE	زمانی‌که هدف ارزیابی به صورت اولیه راه اندازی می‌شود یا بعد از شکست رخ داده، راه اندازی می‌شود، وضعیت امنیتی هدف ارزیابی ممکن است نامعلوم باشد.
T.EAVESDROP	یک کاربر یا پروسه ممکن است داده توابع امنیتی هدف ارزیابی یا کاربری که بین بخش‌های مجزای فیزیکی هدف ارزیابی منتقل می‌شود را مشاهده یا تغییر دهد.

۵,۳ خط‌مشی‌ها

P.TYPE	توضیحات
P.ACCESS_BANNER	هدف ارزیابی باید پرچم اولیه‌های را نمایش دهد که توصیف کننده محدودیت-های استفاده، توافقات قانونی یا هرگونه اطلاعات مناسب دیگری است که کاربران با دستیابی به هدف ارزیابی با آنها موافقت می‌نمایند.
P.ACCOUNTABILITY	کاربران مجاز هدف ارزیابی باید پاسخگوی اقداماتشان در هدف ارزیابی باشند.
P.ADMIN_ACCESS	سرپرستان هدف ارزیابی باید قادر به سرپرستی هدف ارزیابی (محلی و از راه دور) از طریق کانال‌های ارتباطی محافظت شده باشند.
P.COMPATIBILITY	هدف ارزیابی باید الزامات RFC ها را برای پروتکل‌های پیاده‌سازی شده در نظر بگیرد تا با استفاده از این پروتکل‌ها تقابل مسیریاب‌ها را با دیگر تجهیزات شبکه تسهیل کند.
P.VULNERABILITY_ANALYSIS_TEST	هدف ارزیابی باید متحمل تحلیل‌های آسیب‌پذیری مستقل و آزمون نفوذ قرار گیرد تا نشان دهد که هدف ارزیابی نسبت به حملات دارای پتانسیل حمله متوسط مقاوم است.
P.CRYPTOGRAPHY	هدف ارزیابی باید از استاندارد رمزنگاری NIST FIPS به عنوان مبنای همراه با روش‌های تصویب شدهNSA برای مدیریت کلید (یعنی تولید، دسترسی، توزیع، تخریب، بکارگیری و ذخیره کلیدها) و عملیات رمزنگاری (یعنی رمزنگاری، رمزگشایی، امضا، درهم‌سازی، تبادل کلید و تولید اعداد تصادفی) استفاده کند.

۶ اهداف امنیتی

۶,۱ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.ADMIN_ROLE	هدف ارزیابی نقش‌های سرپرستی جهت ایزوله کردن اقدامات سرپرستی و انجام اقدامات سرپرستی را به صورت محلی و از راه دور ارائه خواهد داد.
O.AUDIT_GENERATION	هدف ارزیابی قابلیتی ارائه خواهد داد تا رکوردهایی از رویدادهای امنیتی مربوط به کاربر را شناسایی و ایجاد کند.
O.AUDIT_PROTECTION	هدف ارزیابی قابلیتی ارائه خواهد داد تا از اطلاعات ممیزی محافظت کند.
O.AUDIT_REVIEW	هدف ارزیابی قابلیتی ارائه خواهد داد تا اطلاعات ممیزی به صورت انتخابی مشاهده شود و نسبت به نقص‌های امنیتی بالقوه به سرپرست هشدار دهد.
O.CHANGE_MANAGEMENT	در طول توسعه هدف ارزیابی، پیکربندی هدف ارزیابی و تمام تغییرات اعمال شده به هدف ارزیابی و مدارک توسعه آن از طریق توسعه هدف ارزیابی تحلیل، ردیابی و کنترل خواهد شد.
O.CORRECT_ TSF_OPERATION	هدف ارزیابی جهت اطمینان دادن نسبت به عملکرد صحیح «توابع امنیتی هدف ارزیابی» در محیط عملیاتی‌اش قابلیت آزمون « توابع امنیتی هدف ارزیابی» را ارائه خواهد داد.

O.CRYPTOGRAPHIC_FUNCTIONS	هدف ارزیابی باید عملکرد رمزنگاری (یعنی رمزنگاری/رمزگشایی و عملکرد امضای دیجیتال) را ارائه دهد تا محرمانگی را حفظ کند و برای تشخیص تغییرات داده توابع امنیتی هدف ارزیابی که بین بخش‌های مجزای فیزیکی آن منتقل می‌شوند یا خارج از هدف ارزیابی ذخیره شده‌اند، استفاده شود.
O.DISPLAY_BANNER	هدف ارزیابی یک هشدار مشاوره‌ای در مورد استفاده از هدف ارزیابی را نشان خواهد داد.
O.DOCUMENT_KEY_LEAKAGE	پهنای باند کانالهایی که می‌توانند استفاده شوند تا کلید به خطر بیافتد، باید ثبت شود.
O.MAINT_MODE	هدف ارزیابی باید مودی ارائه دهد که بازیابی یا راه اندازی اولیه رویه‌ها بتواند انجام گیرد.
O.MANAGE	هدف ارزیابی تمام کارکردها و امکانات لازم جهت حمایت مدیران در مدیریت کردن امنیت هدف ارزیابی را ارائه خواهد داد، همچنین استفاده غیرمجاز این کارکردها و امکانات را محدود می‌کند.
O.MEDIATE_INFORMATION_FLOW	هدف ارزیابی باید واسط جریان اطلاعات بین مجموعه‌ای از واسط‌های شبکه هدف ارزیابی یا بین یک واسط شبکه و خود

	هدف ارزیابی مطابق با خط‌مشی هدف ارزیابی قرار گیرد.
O.PEER_AUTHENTICATION	هدف ارزیابی باید هر هدف ارزیابی همتایی را که تلاش در ایجاد رابطه امنیتی با هدف ارزیابی دارد را احرازهویت کند.
O.PROTOCOLS	هدف ارزیابی اطمینان خواهد داد که باتوجه به مشخصه‌های صنعتی/RFC ها، پروتکل‌های استانداردی در هدف ارزیابی پیاده‌سازی می‌شوند تا نسبت به توانایی عملکرد متقابل آن اطمینان حاصل شود.
O.PROTECT_IN_TRANSIT	«توابع امنیتی هدف ارزیابی» باید از داده‌های توابع امنیتی هدف ارزیابی زمانی‌که بین «توابع امنیتی هدف ارزیابی» و دیگر موجودیت‌های مورد اعتماد IT منتقل می‌شود، محاظت کند.
O.REPLAY_DETECTION	هدف ارزیابی امکانی ارائه خواهد داد که تکرار داده احرازهویت و دیگر داده‌های توابع امنیتی هدف ارزیابی و مشخصه‌های امنیتی را تشخیص و رد می‌کند.
O.RESIDUAL_INFORMATION	هدف ارزیابی اطمینان خواهد داد که هیچ یک از داده‌های یک منبع محافظت شده در زمان آزاد سازی آن منبع، در دسترس قرار نخواهند گرفت.
O.RESOURCE_SHARING	هدف ارزیابی باید سازوکارهایی را ارائه دهد تا تلاش‌هایی که در جهت اتمام منابع اتصال محور ارائه شده توسط هدف ارزیابی هستند را کاهش دهد.(برای مثال ورودی‌های یک جدول

	حالت اتصال ، اتصالات TCP به هدف ارزیابی)
O. ROBUST_ADMIN_GUIDANCE	هدف ارزیابی، اطلاعات لازم را برای تحویل و مدیریت امن به سرپرست ارائه خواهد داد.
O.ROBUST_TOE_ACCESS	هدف ارزیابی، سازوکارهایی را ارائه خواهد داد که دسترسی منطقی کاربر به هدف ارزیابی را کنترل می‌کند و در زمان‌های مناسب دسترسی کاربران خاصی را رد می‌کند.
O.SELF_PROTECTION	«توابع امنیتی هدف ارزیابی» یک دامنه برای اجرای خود حفظ می‌کند که خود و منابعش را از مداخلات خارجی، دستکاری‌ها یا افشای غیرمجاز حفظ می‌کند.
O.SOUND_DESIGN	هدف ارزیابی با استفاده از تکنیک‌ها و اصول طراحی قوی طرح‌ریزی خواهد شد. طراحی هدف ارزیابی، اصول طراحی و تکنیک‌های طراحی به طور کامل و دقیق مستند خواهد شد.
O.SOUND_IMPLEMENTATION	پیاده‌سازی هدف ارزیابی نمونه‌ای کامل و دقیق از طراحی‌اش خواهد بود و به طور کامل و دقیق مستند شده است.
O.THOROUGH_FUNCTIONAL_TESTING	هدف ارزیابی تحت آزمون کارکرد امنیتی مناسبی قرار می‌گیرد تا نشان دهد که «توابع امنیتی هدف ارزیابی» الزامات کارکرد امنیتی را برآورده می‌کند.
O.TIME_STAMPS	هدف ارزیابی باید «مهرهای زمانی» معتبری ارائه دهد و به سرپرستان این امکان را بدهد تا زمان مورد استفاده برای این مهرهای زمانی را تنظیم نمایند.

O.TRUSTED_PATH	هدف ارزیابی امکانی ارائه خواهد داد که اطمینان می‌دهد کاربران با سمت مقابلی که تظاهر می‌کند که هدف ارزیابی است، ارتباط برقرار نخواهد کرد.
O.USER_GUIDANCE	هدف ارزیابی اطلاعات لازم برای استفاده صحیح از سازوکارهای امنیتی را در اختیار کاربران قرار می‌دهد.
O.VULNERABILITY_ANALYSIS_TEST	هدف ارزیابی باید متحمل تحلیل‌های آسیب‌پذیری مستقل و آزمون نفوذ قرار گیرد تا نشان دهد که هدف ارزیابی به حملات دارای پتانسیل حمله متوسط اجازه نقض کردن خط‌مشی‌های امنیتی را نمی‌دهد.

۶,۲ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.NO_GENERAL_PURPOSE	به غیر از سرویس‌های لازم برای عملیات، سرپرستی و پشتیبانی هدف ارزیابی، هیچ قابلیت محاسباتی همه منظوره (برای مثال کامپایلرها ، ویرایش‌گرها یا برنامه‌های کاربردی) که بر روی هدف ارزیابی در دسترس باشند، وجود ندارد.
OE.PHYSICAL	امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌های آن، توسط محیط IT

	ارائه می‌شود.
OE.AVAILABILITY	منابع شبکه در دسترس خواهند بود تا به کلاینت‌ها برای برآورده کردن الزامات ماموریت و انتقال اطلاعات، اجازه دهند.

۷ الزامات کارکرد امنیتی مسیریاب‌های شبکه

در این بخش به بررسی کلاس‌ها، خانواده‌ها و الزامات امنیتی پرداخته شده است. استفاده از توابع، الگوریتم‌ها و ماژول‌های بومی که در مقایسه با معادل‌های استاندارد جهانی، به تایید نهادهای بالاسری مربوطه رسیده باشند، در اجرای عملیات ارزیابی امتیاز بالاتری خواهند داشت.

۷,۱ کلاس ممیزی امنیت

در ادامه المان‌های امنیتی مورد نیاز کلاس ممیزی امنیت ارائه شده است.

نام کلاس: ممیزی امنیت

شرح کلاس: سیستم‌های تشخیص نفوذ برای رخدادهای گوناگون اقدام به ایجاد گزارش‌هایی برای ممیزی می‌نمایند. کلاس ممیزی امنیتی، الزاماتی پیرامون نحوه شناخت، ثبت و ذخیره و آنالیز اطلاعات ممیزی مربوط به فعالیت‌های مرتبط امنیتی ارائه می‌کند (فعالیت‌هایی که توسط توابع امنیتی هدف ارزیابی کنترل می‌شوند). با بررسی ممیزی‌های ثبت شده می‌توان تعیین کرد که کدام رخداد، با چه فعالیت امنیتی صورت گرفته مرتبط است و چه‌کسی (چه کاربری) مسوول آن است. این کلاس شامل ۶ خانواده است که عبارتند از:

- **خانواده پاسخ خودکار ممیزی امنیت[1]:**

این خانواده واکنش‌های لازم را هنگام کشف رخدادهایی که دلالت بر نقض امنیتی بالقوه‌ای دارند، تعریف می‌کند.

- **خانواده تولید داده ممیزی[1]:**

1 Security audit automatic response (FAU_ARP)

این خانواده الزاماتی را برای ثبت رخدادهای امنیتی مربوط به رویدادهایی که تحت کنترل توابع امنیتی هدف ارزیابی صورت می‌گیرند را تعریف می‌کند. این خانواده سطح ممیزی را تعیین می‌کند، هم‌چنین انواع رویدادهایی که بایستی توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند را بیان می‌کند و یک مجموعه حداقلی از اطلاعات مرتبط با ممیزی را تعیین می‌کند که باید در داخل انواع ممیزی‌های امنیتی ثبت شده، ارائه شوند.

- **خانواده تحلیل ممیزی امنیت[۲]:**

این خانواده الزاماتی برای ابزارهای خودکار، که فعالیت‌های سیستم را تحلیل می‌نمایند و داده‌های ممیزی که نقض امنیتی واقعی یا ممکن را جستجو می‌کنند، تعریف می‌کند. این تحلیل ممکن است در پشتیبانی از تشخیص نفوذ، یا پاسخ خودکار به نقض امنیتی بالقوه کار کند.

- **خانواده بازبینی ممیزی امنیت[۳]:**

این خانواده تعریف کننده الزاماتی برای ابزارهای ممیزی است که باید در دسترس کاربران مجاز قرار بگیرد تا به بازبینی داده‌های ممیزی کمک کند.

- **خانواده انتخاب رویداد ممیزی امنیت[۴]:**

این خانواده تعریف کننده الزاماتی جهت انتخاب یک مجموعه رویدادهای ممیزی شده در طول عملکرد هدف ارزیابی، از بین تمام رویدادهای قابل ممیزی می‌باشد.

---

1 Security audit data generation (FAU_GEN)

2 Security audit analisys (FAU_SAA)

3 Security audit review (FAU_SAR)

4 Security audit event selection (FAU_SEL)

- **خانواده ذخیره‌سازی رویداد ممیزی امنیت**[1]:

این خانواده تعریف کننده الزاماتی برای توابع امنیتی هدف ارزیابی است تا قادر به ایجاد و نگهداری از سوابق ممیزی بصورت امن باشد.

1 Security audit event storage (FAU_STG)

۷,۲ کلاس پشتیبانی از رمزنگاری

در ادامه المان‌های امنیتی مورد نیاز کلاس پشتیبانی از رمزنگاری ارائه شده است.

نام کلاس: پشتیبانی از رمزنگاری

شرح کلاس: توابع امنیتی هدف ارزیابی ممکن است با به کار بردن قابلیت‌های رمزنگاری، به ارضاء شدن چندین هدف امنیتی سطح بالا کمک نمایند: این اهداف می‌تواند شامل موارد زیر باشد، اما تنها به این دسته نیز محدود نمی‌شود:

- شناسایی و احراز هویت
- عدم انکار
- مسیر امن
- کانال امن
- مجزاسازی داده

این کلاس زمانی که هدف ارزیابی، عملکرد رمزنگاری را پیاده‌سازی می‌کند، استفاده می‌شود رمزنگاری پیاده‌سازی شده در نرم‌افزار، سخت‌افزار و میان افزار می‌تواند صورت گیرد.

- **خانواده مدیریت کلید رمزنگاری**

کلیدهای رمزنگاری باید از طریق دوره حیاتشان مدیریت شوند. این خانواده برای پشتیبانی از دوره حیات کلید در نظر گرفته می‌شود و درنتیجه الزاماتی را برای فعالیت‌های زیر تعریف می‌کند:

- تولید کلید رمزنگاری
- توزیع کلید رمزنگاری
- دستیابی به کلید رمزنگاری
- تخریب کلید رمزنگاری

در صورت وجود الزامات عملیاتی برای مدیریت کلیدهای رمزنگاری، این خانواده نیز باید در نظر گرفته شود.

- **خانواده عملیات رمزنگاری**

به منظور عملکرد صحیح عملیات رمزنگاری، این عملیات باید مطابق با الگوریتم خاص و کلید رمزنگاری با اندازه مشخص انجام گیرد. در صورت وجود الزامات عملیاتی برای مدیریت کلیدهای رمزنگاری، این خانواده نیز باید در نظر گرفته شود.

معمولاً عملیات رمزنگاری شامل رمزنگاری و رمزگشایی داده، تائید و/یا تولید امضای دیجیتال، تولید کنترل [1]رمزنگاری برای یکپارچگی و صحت یا تائید کنترل، درهم‌سازی امن (خلاصه پیام)، رمزنگاری و/یا رمزگشایی کلید رمزنگاری، و توافق کلید رمزنگاری می‌باشد.

۷,۳ کلاس حفاظت از داده‌های کاربری

در ادامه المان‌های امنیتی مورد نیاز کلاس حفاظت از داده‌های کاربری ارائه شده است.

نام کلاس: حفاظت از داده کاربری

1 Checksum

شرح کلاس: این کلاس شامل خانواده‌هایی است که الزامات مربوط به محافظت از داده کاربر را مشخص می‌نمایند: این کلاس شامل ۱۳ خانواده است که در چهار گروه زیر دسته‌بندی شده‌اند، که داده‌های کاربری در داخل هدف ارزیابی، در طول ورود، خروج و ذخیره سازی آدرس‌دهی می‌کنند هم‌چنین صفات امنیتی را مستقیماً به داده کاربری مرتبط می‌کند.

خانواده‌های این کلاس در چهار گروه زیر دسته‌بندی شده‌اند:

۱) خط‌مشی‌های عملکرد امنیتی مربوط به محافظت از داده کاربری
- خط‌مشی‌های کنترل دسترسی (ح‌ف-س‌ک)[1]
- خط‌مشی‌های مرتبط با کنترل جریان اطلاعات (ح‌ف-خ‌ج)[2]

عناصر این خانواده‌ها به نویسنده هدف امنیتی/پروفایل حفاظتی اجازه می‌دهند تا خط‌مشی‌های عملکرد امنیتی مربوط به حفاظت از داده کاربری را نام ببرند و حوزه کنترلی خط‌مشی‌ها را تعریف نموده و در صورت لزوم اهداف امنیتی را آدرس‌دهی نمایند. نام بردن خط‌مشی‌ها در این دو خانواده بدین منظور است که باقی عناصر عملیاتی، با استفاده از قسمت «اختصاص» و «انتخاب» بتوانند سیاست‌گذاری‌های مطرح شده در دو خانواده

- سیاست‌گذاری‌های عملکرد امنیتی کنترل دستیابی
- سیاست‌گذاری‌های عملکرد امنیتی کنترل جریان اطلاعات

را فراخوانی نمیاند.

1 Access control policy(FDP_ACC)

2 Information flow control policy(FDP_IFC)

قوانین، تعریف عملکرد سیاست‌گذاری‌های مطرح شده در این دو خانواده درخانواده‌های توابع کنترل دسترسی (حف-ت‌ک)[1] و توابع کنترل جریان اطلاعات (حف-ک‌ج)[2] تعریف خواهد شد.

۲) فرم‌های مختلف محافظت از داده کاربری

- توابع کنترل دسترسی (حف-ت‌ک)
- توابع کنترل جریان اطلاعات (حف-ک‌ج)
- انتقال هدف ارزیابی داخلی (حف-اد)[3]
- حفاظت از اطلاعات باقیمانده (حف-اب)[4]
- عملیات عقب‌گرد به منظور بازگرداندن حالت/حالت‌های قبل (حف-ع‌گ)[5]
- یکپارچگی داده‌های ذخیره شده (حف-ی‌د)[6]

۳) ارسال، دریافت و ذخیره داده به صورت برون‌خطی[7]

- تصدیق اصالت[8] داده (حف-ت‌د)

---

1 Access control functions(FDP_ACF)

2 Information flow control functions(FDP_IFF)

3 Internal TOE transfer(FDP_ITT)

4 Residual information protection(FDP_RIP)

5 Rollback(FDP_ROL)

6 Stored data integrity(FDP_SDI)

7 Offline

8 Data authentication(FDP_DAU)

- صادر شده از هدف ارزیابی (حف-ص‌ا)[1]
- ورود داده‌ها از بیرون به هدف ارزیابی (حف-وب)[2]

عناصر این خانواده‌ها، انتقال داده در داخل یا خارج از هدف ارزیابی را به صورت قابل اطمینانی آدرس‌دهی می‌نمایند.

۴) ارتباطات در داخل توابع امنیتی هدف ارزیابی

- محافظت از انتقال محرمانگی داده کاربر در توابع امنیتی هدف ارزیابی داخلی(حف-م‌د)[3]
- محافظت از انتقال یکپارچگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-ی‌ا)[4]

مؤلفه‌های این خانواده ارتباطات بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن فناوری اطلاعات را آدرس‌دهی می‌کند.

➢ خانواده خط‌مشی‌های کنترل دسترسی

این خانواده خط‌مشی‌های عملکرد امنیتی مربوط به کنترل دسترسی (توسط نام) را معرفی می‌کند و حوزه کنترلی خط‌مشی‌ها را تعریف می‌کند به گونه‌ای که بخش کنترل دسترسی مشخص شده، الزام عملکرد امنیتی مربوط به خط‌مشی عملکرد امنیتی باشد. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال[5] تحت کنترل سیاست‌گذاری‌ها
- موجودیت‌های غیرفعال[1] تحت کنترل سیاست‌گذاری‌ها

---

1 Export from the TOE(FDP_ETC)

2 Import from outside of the TOE(FDP_ITC)

3 Inter-TSF user data confidentiality transfer protection(FDP_UCT)

4 Inter-TSF user data integrity transfer protection(FDP_UIT)

5 Subject

– عملیات بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده که توسط این خط‌مشی‌ها پوشش داده می‌شود.

معیارهای مطرح شده، اجازه می‌دهد چندین خط‌مشی با نام‌های منحصر به فردی وجود داشته باشد.

قوانینی که تعریف‌کننده خط‌مشی‌های عملکرد کنترل دسترسی می‌باشد، در دیگر خانواده‌های این کلاس هم‌چون توابع کنترل دسترسی (ح‌ف-ت‌ک) و ارسال از هدف ارزیابی (ح‌ف-ص‌ا) تعریف می‌شوند.

سیاست‌گذاری‌های عملکرد امنیتی کنترل دسترسی در این خانواده نام برده شده است، تا دیگر عناصر عملیاتی از این سیاست‌گذاری‌ها در قسمت «انتخاب» یا «اختصاص» استفاده نمایند.

➢ خانواده توابع کنترل دسترسی

این خانواده توصیف کننده قوانینی برای توابع خاص است که می‌تواند خط‌مشی‌های کنترل دسترسی را که در خانواده خط‌مشی کنترل دسترسی (ح‌ف-س‌ک) نام برده شده است، پیاده‌سازی کند. خانواده خط‌مشی کنترل دسترسی (ح‌ف-س‌ک) حوزه کنترل سیاست‌گذاری را نیز مشخص می‌کند.

➢ خانواده تصدیق اصالت داده

خانواده تصدیق اصالت داده به هر نهادی، اجازه بررسی صحت اطلاعات را می‌دهد (با امضای دیجیتالی کردن اطلاعات). این خانواده روشی را مشروط بر تضمین اعتبار یک

---

1 Object

بخش خاص از داده ارائه می‌کند که می‌تواند به منظور بررسی محتوای اطلاعات از لحاظ جعل نشدن یا تغییر یافتن به صورت مکرر مورد استفاده قرار گیرد. در مقابل کلاس ممیزی امنیتی برای داده‌های ایستا در نظر گرفته شده است.

- **خانواده صادرشده از هدف ارزیابی**

در این خانواده عملکردهایی برای ارسال داده کاربری توسط هدف ارزیابی بین توابع امنیتی هدف ارزیابی، تعریف شده است بطوری‌که صفات امنیتی و حفاظت می‌تواند به صراحت در هنگام ارسال داده حفظ شود یا نادیده گرفته شود. این خانواده بر روی ارسال داده محدودیت‌هایی اعمال می‌کند و صفات امنیتی را به داده کاربری ارسال شده، اختصاص می‌دهد.

- **خط‌مشی‌های کنترل جریان اطلاعات**

این خانواده سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات را معرفی می‌کند (با نام) و برای هریک از آنها، حوزه کنترلی را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال تحت کنترل سیاست‌گذاری‌ها
- اطلاعات تحت کنترل سیاست‌گذاری‌ها
- عملیاتی که سبب کنترل اطلاعات جریان یافته به/از موجودیت‌های فعال کنترل شده تحت پوشش این خط‌مشی‌ها می‌باشند.

معیارهای مطرح شده، اجازه می‌دهد چندین خط‌مشی با نام‌های منحصر به فردی وجود داشته باشد.

قوانینی تعریف کننده سیاست‌گذاری‌های عملکرد جریان اطلاعات، توسط خانواده‌های دیگر هم‌چون توابع کنترل دسترسی (حف-ت‌ک) و صدور داده از هدف ارزیابی (حف-

ص‌ا) تعریف می‌شوند.

نام بردن سیاست‌گذاری‌های عملکرد امنیتی کنترل دسترسی به منظور استفاده از باقی مؤلفه‌های عملیاتی[1] است که دارای عملیاتی هستند که در قسمت «انتخاب» یا «اختصاص» مربوط به سیاست‌گذاری‌های عملکرد امنیتی کنترل جریان اطلاعات فراخوانی می‌شود.

سازوکار توابع امنیتی هدف ارزیابی، جریان اطلاعات را مطابق با سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات، کنترل می‌کند. عملیاتی که مشخصه-های امنیتی اطلاعات را تغییر می‌دهند به طورکلی مجاز به نقض سیاست‌گذاری‌های عملکرد امنیتی کنترل جریان اطلاعات نمی‌باشند. چنین عملیاتی اگر به صراحت ذکر شوند، ممکن است به عنوان یک استثناء برای کنترل جریان اطلاعاتی مربوط به سیاست‌گذاری‌های عملکرد امنیتی در نظر گرفته شوند.

- **خانواده توابع کنترل جریان اطلاعات**

این خانواده توصیف کننده قوانینی برای عملکردهای خاصی است که می‌تواند سیاست‌گذاری‌های عملکرد امنیتی کنترل جریان اطلاعات که در خانواده حف-خج ذکر شده است را پیاده سازی کند، هم‌چنین حوزه کنترلی سیاست‌گذاری را مشخص می‌کند. این خانواده شامل دو الزام است:

- پرداختن به مسائل عملکرد جریان اطلاعات رایج
- پرداختن به جریان اطلاعات غیرمجاز

این تقسیم‌بندی به این دلیل مطرح شده است که مسائل مربوط به جریان اطلاعات غیرمجاز، در برخی موارد با بقیه سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات در تعامد است. با توجه به طبیعتشان در اثر تخلف از خط‌مشی‌ها، آنها از سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات سرپیچی می-

1 Functional component

نمایند. به عنوان مثال، آنها به توابع خاصی نیاز دارند تا وقوع آنها را محدود یا از آن جلوگیری کند.

- **خانواده ورود داده‌ها از بیرون به هدف ارزیابی**

این خانواده تعریف کننده سازوکارهایی برای دریافت داده کاربری در داخل هدف ارزیابی است، به گونه‌ای که این داده صفات امنیتی مناسبی داشته باشد و هم‌چنین به اندازه کافی محافظت شده باشد. این خانواده با اعمال محدودیت بر روی داده، تعیین صفات امنیتی مطلوب و تفسیر صفات امنیتی مربوط به کاربر در ارتباط است.

- **خانواده انتقال هدف ارزیابی داخلی**

این خانواده الزاماتی را ارائه می‌دهد تا از داده کاربری در زمانی‌که بین بخش‌های مجزای هدف ارزیابی در سراسر کانال‌های داخلی انتقال می‌یابد، حفاظت کند. این امر ممکن است با خانواده‌های «محافظت از انتقال محرمانگی داده کاربر کارکرد امنیتی هدف ارزیابی داخلی (حف-مد)» و «محافظت از انتقال یکپارچگی داده کاربر کارکرد امنیتی هدف ارزیابی داخلی(حف-ی‌ا)» در تضاد باشد، این خانواده‌ها از داده‌های کاربری در زمانی‌که بین توابع امنیتی هدف ارزیابی مجزا در سراسر یک کانال خارجی انتقال می‌یابد، حفاظت می‌نمایند. هم‌چنین خانواده‌های «صدور داده از هدف ارزیابی (حف-ص‌ا)» و «ورود داده از بیرون به هدف ارزیابی (حف-وب)» که انتقال داده در میان توابع امنیتی هدف ارزیابی که از خارج هدف ارزیابی دریافت شده‌اند یا از داخل هدف ارزیابی ارسال می‌شوند را آدرس‌دهی می‌کند.

- **خانواده حفاظت از اطلاعات باقیمانده**

این خانواده اطمینان می‌دهد، زمانی‌که منبع از یک موجودیت غیرفعال آزاد می‌شود و دوباره به یک موجودیت غیرفعال دیگر اختصاص داده می‌شود، در این صورت هرگونه

داده موجود در منبع غیرقابل دسترس شود. هم‌چنین این خانواده ملزم می‌کند که هر داده موجود در منبع که به طور منطقی حذف یا آزاد می‌شود، محافظت شود، زیرا ممکن است این داده هنوز در داخل توابع امنیتی هدف ارزیابی کنترل شده که به موجودیت غیرفعال دیگری اختصاص یافته است، وجود داشته باشد.

- **خانواده عملیات عقب‌گرد به منظور بازگرداندن حالت/ حالت‌های قبل**

عملکرد عقب‌گرد شامل بی‌اثر کردن آخرین عملکرد یا یک سری از عملکردها، محدود شدن به برخی محدودیت‌ها هم‌چون بازه زمانی و برگشت به یک وضعیت شناخته شده قبلی می‌باشد. عقب‌گرد فراهم کننده قابلیت بی‌اثر کردن عملیات یا مجموعه‌ای از عملیات است تا یکپارچگی داده کاربری را حفظ کند.

- **خانواده یکپارچگی داده‌های ذخیره شده**

این خانواده در برگیرنده الزاماتی است که از داده کاربری ذخیره شده در کانتینر که توسط توابع امنیتی هدف ارزیابی کنترل می‌شود، محافظت می‌کند. خطای یکپارچگی ممکن است داده کاربری ذخیره شده در حافظه یا در یک ابزار ذخیره‌سازی را تحت تاثیر قرار دهد. این خانواده متفاوت از خانواده «انتقال هدف ارزیابی داخلی (ح‌ف-اد)» است که داده کاربری را در حالی‌که داخل هدف ارزیابی انتقال می‌یابد از خطاهای یکپارچگی محافظت می‌کند.

- **خانواده محافظت از انتقال محرمانگی داده کاربر در توابع امنیتی هدف ارزیابی داخلی**

این خانواده تعریف کننده الزاماتی است که محرمانگی داده کاربری را در زمانی‌که با استفاده از یک کانال خارجی بین هدف ارزیابی و دیگر محصولات امن IT انتقال می‌یابد، تضمین می‌کند.

➢ خانواده محافظت از انتقال یکپارچگی داده کاربر در کارکرد امنیتی هدف ارزیابی داخلی

این خانواده الزاماتی را تعریف می‌کند تا یکپارچگی داده کاربری را که بین هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شود، تامین کند و از خطاهای قابل تشخیص بازیابی شود. حداقل این خانواده، یکپارچگی داده کاربری را برای تغییرات نظارت می‌کند. همچنین، این خانواده از روش‌های مختلف اصلاح خطاهای یکپارچگی تشخیص داده شده، نیز پشتیبانی می‌کند.

شماره الزام	نام خانواده	عنصر امنیتی
۱	**حفاظت از اطلاعات باقیمانده (FDP_RIP)**	**نام عنصر: حفاظت کامل از اطلاعات باقیمانده ۲** **شماره مؤلفه: ح‌ف-اب.۱,۲ (FDP_RIP.2.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تضمین کند که هرگونه محتوای اطلاعات قبلی یک منبع در زمان [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت های غیرفعال، غیرقابل دسترس می‌باشد.
۲	خط‌مشی‌های مرتبط	**نام عنصر: کنترل زیرمجموعه جریان اطلاعات(خط‌مشی نامعتبر) ۱(۱)**

شماره الزام	نام خانواده	عنصر امنیتی
با کنترل جریان اطلاعات (FDP_IFC)		**شماره مؤلفه: ح‌ف-خ‌ج.۱،۱(۱) ((FDP_IFC.1.1(1))**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعات نامعتبر] بر روی [

- موجودیت فعال مبدا: واسط[1] هدف ارزیابی که اطلاعات بر روی آن دریافت می‌شود.
- موجودیت فعال مقصد: واسط هدف ارزیابی که اطلاعات به آن می‌رسد.
- اطلاعات: بسته‌های شبکه، نمونه‌ای از اطلاعات هستند.
- عملیات: عبور اطلاعات به وسیله باز کردن یک اتصال رله از طریق توابع امنیتی هدف ارزیابی از طرف موجودیت فعال مبدأ به موجودیت فعال مقصد و با حصول اطمینان از شرایط زیر:
  - اتصال از موجودیت فعال مبدأ که در یک شبکه معتبر متناظر است.
  - اتصال رله جدید که به سمت موجودیت فعال مقصد روی یک شبکه معتبر متناظر، ساخته می‌شود.]

اجرا کند.

1 Interface

شماره	نام خانواده	عنصر امنیتی
الزام		
۳		**نام عنصر: کنترل زیرمجموعه جریان اطلاعات(خط‌مشی نامعتبر) ۱(۲)**
		شماره مؤلفه: ح‌ف-خ‌ج.۱,۱(۲) ((FDP_IFC.1.1(2))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعات معتبر] بر روی [
		• موجودیت فعال مبدا به نمایندگی از مسیریاب‌های همتای معتبر: شناسه شبکه مبدا
		• موجودیت فعال مقصد: واسط هدف ارزیابی که اطلاعات به آن می‌رسد.
		• اطلاعات: بسته‌های شبکه، نمونه‌ای از اطلاعات هستند.
		• عملیات: عبور اطلاعات به وسیله باز کردن یک اتصال رله از طریق توابع امنیتی هدف ارزیابی از طرف موجودیت فعال مبدأ به موجودیت فعال مقصد و با حصول اطمینان از شرایط زیر:
		○ اتصال از موجودیت فعال مبدأ که در یک شبکه معتبر متناظر است.
		○ اتصال رله جدید که به سمت موجودیت فعال مقصد روی یک شبکه معتبر متناظر، ساخته می‌شود.]
		اجرا کند.

شماره	نام خانواده	عنصر امنیتی
الزام		
۴	عملیات کنترل جریان اطلاعات (FDP_IFF)	**نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی نامعتبر) (۱)** **شماره مؤلفه: ح‌ف-ک‌ج.۱,۱(۱)(۱)(FDP_IFF.1.1(1))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعات نامعتبر] براساس انواع موجودیت‌های فعال و مشخصه‌های امنیتی اطلاعات زیر را اجرا کند: ۱. [مشخصه امنیتی موجودیت فعال مبدا: • مجموعه‌ای از شناسه‌های موجودیت مبدا؛ و • [انتخاب: [اختصاص: دیگر مشخصه‌های امنیتی موجودیت‌های فعال]، هیچکدام] ۲. مشخصه‌های امنیتی موجودیت فعال مقصد: • مجموعه‌ای از شناسه‌های موجودیت مقصد؛ و • [انتخاب: [اختصاص: دیگر مشخصه‌های امنیتی موجودیت فعال]، هیچکدام]. **نکته کاربردی:**

شماره **نام خانواده**

الزام

عنصر امنیتی

برای موجودیت‌ها، سرپرست از مجموعه‌ای شناسه‌ها که می‌توانند به واسط مسیریاب فیزیکی مرتبط شوند، آگاهی دارد. بنابراین این دسته از شناسه‌ها جزء شناسه‌های فرضی به حساب نمی‌آیند. اصطلاح «شناسه» به جای «آدرس» استفاده می‌شود، تا به فناوری‌هایی که مبتنی برآدرس نیستند نیز امکان مرتبط شدن با واسط مسیریاب فیزیکی را بدهند (برای مثال، شناسه مدار به جای آدرس مبدا و مقصد).

نویسنده هدف امنیتی باید دیگر مشخصه‌هایی که در شناسایی مجموعه موجودیت‌های مبدا و مقصد استفاده می‌شوند را بر اساس فناوری پیاده‌سازی شده توسط هدف ارزیابی مشخص کند.

۳. مشخصه‌های امنیتی اطلاعات

- هویت فرضی موجودیت مبدا
- هویت موجودیت مقصد
- پروتکل لایه انتقال
- شناسه سرویس موجودیت مبدا
- شناسه سرویس موجودیت مقصد (برای مثال، شماره پورت مقصد TCP یا UDP)

نکته کاربردی:

شماره **نام خانواده**

الزام

عنصر امنیتی

پروتکل لایه انتقال همانند سرآیند IP است که در فیلد پروتکل ۸ بیتی مشخص شده است (برای مثال می‌تواند شامل ICMP باشد و به TCP یا UDP محدود نشود). مفهوم «شناسه سرویس» ممکن است با توجه به پشته شبکه مورد استفاده متفاوت باشد. هدف مشخص کردن سرویسی است که در پشته پروتکل بالای لایه انتقال و شبکه باشد. یک سرویس همانند NTP، [1] TFTP و غیره.

نکته کاربردی:

تمام صفات امنیتی ذکر شده در بالا، لازم نیست که در تمام بسته‌های شبکه وجود داشته باشند. هرچند مجموعه قوانین هدف ارزیابی، به سرپرست امنیتی این اجازه را می‌دهد تا هریک از صفات امنیتی به عنوان بخشی از تصمیم سیاست‌گذاری را انتخاب و فیلتر کند.

منظور آن است که اگر یک بسته شبکه، شامل هیچ کدام از صفات امنیتی بالا نباشد، از آن صفات ممکن است در تصمیمات سیاست-گذاری استفاده شود. نویسنده هدف امنیتی، باید قسمت «اختصاص» را با تمام صفاتی تکمیل کند که سرپرست امنیتی در زمان ایجاد قوانین مسیریاب، قادر به مشخص کردن آنها باشد.

برای پشته‌های شبکه مبتنی بر غیر IP : [اختصاص: صفات امنیت اطلاعات]

].

1 Trivial File Transfer Protocol

شماره	نام خانواده	عنصر امنیتی
الزام		

نکته کاربردی:

در صورتی‌که هدف ارزیابی، از پشته شبکه مبتنی بر IP استفاده کند (شامل اجرای IP بر روی پروتکل‌های دیگر، همچون حالت انتقال غیرهمزمان (ATM))، در قسمت «انتخاب» الزام بالا، اولین مورد انتخاب می‌شود.

اگر هدف ارزیابی، از پشته شبکه مبتنی بر غیر IP استفاده کند (برای مثال ATM بدون IP)، بنابراین نویسنده هدف امنیتی دومین مورد را در قسمت «انتخاب» الزام بالا، انتخاب می‌کند و قسمت «اختصاص» را با صفاتی تکمیل می‌کند تا برای پروتکل‌های به کار رفته سطح قابل قبولی از اطمینان را ارائه دهد تا بسته‌های شبکه بتوانند به درستی با یک اتصال مرتبط شوند.

۵ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی نامعتبر) (۱)**

شماره مؤلفه: ح‌ف-ک‌ج.۲,۱(۱)((FDP_IFF.1.2(1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مجوز جریان اطلاعات بین موجودیت‌های فعال مبدا و اطلاعات کنترل شده را از طریق عملیات‌های کنترل شده، توسط قانون زیر را فراهم آورند:

- [هویت فرضی موجودیت مبدا، در مجموعه‌ای از شناسه‌های موجودیت مبدا می‌باشد؛

شماره **نام خانواده**

الزام

عنصر امنیتی

- هویت موجودیت مقصد در مجموعه‌ای از شناسه‌های موجودیت مقصد می‌باشد؛
- مشخصه‌های امنیت اطلاعات با توجه به الگوریتم‌های [اختصاص: الگوریتم‌هایی که توسط هدف ارزیابی جهت منطبق کردن مشخصه‌های امنیت اطلاعات با قوانین سیاست‌گذاری اطلاعات استفاده می‌شود] منطبق بر صفات در قوانین سیاست‌گذاری جریان اطلاعات می‌باشد.
- قانون سیاست‌گذاری جریان اطلاعات که انتخاب شده است، مجاز بودن جریان اطلاعات را مشخص می‌کند].

نکته کاربردی:

در مسیریاب، قوانین خط‌مشی جریان اطلاعات توسط سرپرست مشخص می‌شود که این قوانین شامل مقادیر مربوط به صفات امنیتی اطلاعات می‌باشند (یا علامت‌های عمومی که برای مقادیر مختلف «ایستاده» می‌باشد؛ برای مثال آدرس 127.*.*.* هر آدرس IP که با 127 شروع می‌شود را نشان می‌دهد.) و به هر قانون یک اقدام مرتبط شده است که یا اجازه جریان یافتن اطلاعات را می‌دهد یا جریان یافتن اطلاعات را غیرمجاز می‌کند. زمانی‌که یک بسته به واسط مبدا رسید، مقادیر صفات امنیتی اطلاعات آن بسته توسط برخی از الگوریتم‌های مشخص هدف ارزیابی با هر یک از قوانین سیاست‌گذاری جریان اطلاعات مقایسه می‌شود و در صورت منطبق بودن، اقدام مشخص شده توسط قانون صورت می‌گیرد.

شماره	نام خانواده	عنصر امنیتی
الزام		

از آنجا که علامت عمومی اجازه می‌دهد صفات خاص در یک بسته، به طور بالقوه با بیش از یک قانون مطابق باشد، نویسنده هدف امنیتی نیاز دارد تا قسمت «اختصاص» را با الگوریتمی کامل گرداند که هدف ارزیابی برای یافتن « قانون منطبق» از آن استفاده می‌کند.

این می‌تواند «اولین تطابق»، « خاص‌ترین تطابق» یا شامل توضیحات مفصل‌تری باشد.

۶ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی نامعتبر) (۱)**

شماره مؤلفه: ح‌ف-ک‌ج.۳,۱(۱)((FDP_IFF.1.3(1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [اختصاص: قوانین اضافی کنترل جریان اطلاعات] را اجرا کند.

۷ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی نامعتبر) (۱)**

شماره مؤلفه: ح‌ف-ک‌ج.۴,۱(۱)((FDP_IFF.1.4(1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید موارد زیر را ارائه کند [سرپرست امنیتی باید پیش از بکار بردن مجموعه قوانین بتواند تمام جریان اطلاعاتی که توسط مجموعه قوانین سیاست‌گذاری جریان اطلاعات مجاز شده است را مشاهده کند]

شماره	نام خانواده	عنصر امنیتی
الزام		

نکته کاربردی:

در اثر ایجاد یک قانون، برخی مسیریاب‌ها قوانین بیشتری نیز تولید می‌کنند؛ برای مثال، یک مسیریاب ممکن است در زمان ایجاد قانون مجاز FTP (کنترل اتصالات)، قانون مجاز کانال داده FTP را ایجاد کند. این الزام به سرپرست اجازه می‌دهد تا تمام مجموعه قوانین را مشاهده کند، تا بتواند این قواینن را شناسایی نموده و تائید کند که این مجموعه قوانین، منعکس کننده خط‌مشی مورد نظر است.

منظور از عبارت « پیش از بکار بردن مجموعه قوانین» ، آن است که پیش از آنکه قوانین روی هدف ارزیابی اعمال شود، سرپرست قادر به مشاهده تمام مجموعه قوانین باشد و هم‌چنین به سرپرست این فرصت را می‌دهد تا هر خطا یا جریان ناخواسته را نشان دهد.

۸ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی نامعتبر) (۱)**

شماره مؤلفه: ح‌ف-ک‌ج.۵,۱(۱)(FDP_IFF.1.5(1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید صریحاً اجازه جریان یافتن اطلاعات مبتنی بر قوانین زیر را بدهد: [هیچکدام]

۹ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی نامعتبر) (۱)**

شماره مؤلفه: ح‌ف-ک‌ج.۶,۱(۱)(FDP_IFF.1.6(1))

شماره **نام خانواده**

الزام

عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید صریحاً جریان یافتن اطلاعاتی مبتنی بر قوانین زیر را انکار کند:

- [درصورتی که شناسه مبدأ مفروض اطلاعات دریافتی از هدف ارزیابی در مجموعه شناسه‌های موجودیت فعال مبدأ نباشد، هدف ارزیابی باید مانع از درخواست‌های دسترسی یا ارائه سرویس شود.

نکته کاربردی:

منظور این الزام آن است تا اطمینان حاصل شود که کاربر نمی‌تواند بسته‌هایی که ادعای ایجاد شدن بر روی یک واسط هدف ارزیابی دیگری را دارند ، بر روی واسطی ارسال کند که بر روی آن ایجاد شده است.

- درصورتی که شناسه مبدأ فرض شده از اطلاعات دریافتی توسط هدف ارزیابی یک شناسه Broadcast باشد، هدف ارزیابی باید مانع از درخواست‌های دسترسی یا ارائه سرویس شود.

نکته کاربردی:

شناسه‌ایی Broadcast است که بیش از یک آدرس میزبان را بر روی شبکه مشخص کند. بدیهی است که هدف ارزیابی می‌تواند تنها از پیکربندی زیرشبکه‌ای از شبکه‌هایی که به طور مستقیم به واسط هدف ارزیابی متصل هستند، آگاهی یابد و در نتیجه تنها از آدرس‌های

شماره الزام	نام خانواده	عنصر امنیتی

Broadcast در این شبکه‌ها مطلع می‌شود.

- درصورتی که شناسه مبدأ مفروض اطلاعات دریافتی توسط هدف ارزیابی یک شناسه Loopback باشد، هدف ارزیابی باید مانع از درخواست‌های دسترسی یا ارائه سرویس شود.
- در صورتی‌که اطلاعات دریافتی توسط هدف ارزیابی شامل مسیری[1](مجموعه‌ای از شناسه‌های شبکه میزبان) باشد که توسط اطلاعات باید از موجودیت فعال مبدا به سمت موجودیت فعال مقصد جریان یابد، هدف ارزیابی باید مانع از درخواست شود].

۱۰ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی معتبر) (۲)**

شماره مؤلفه: ح‌ف-ک‌ج.۱,۱(۲)((FDP_IFF.1.1(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی مربوط به جریان اطلاعات معتبر] براساس انواع مشخصه‌های امنیتی موجودیت-های فعال و اطلاعاتی که در زیر مطرح شده است را اجرا کند:

۴. [مشخصه امنیتی موجودیت فعال مبدا:

1 Route

شماره نام خانواده

الزام

عنصر امنیتی

- شناسه شبکه مبدا
- [انتخاب: [اختصاص: دیگر مشخصه‌های امنیتی موجودیت‌های فعال]، هیچکدام]

نکته کاربردی:

توجه شود که در بالا نیازی به مشخص کردن «شناسه کاربری» برای استفاده در قانون سیاست‌گذاری جریان اطلاعات نمی-باشد. اگر هدف ارزیابی این ویژگی را ارائه کند لازم است تا در بولت دوم ذکر شود.

۵. مشخصه‌های امنیتی موجودیت فعال مقصد:

- مجموعه‌ای از شناسه‌های شبکه مقصد؛ و
- [انتخاب: [اختصاص: دیگر مشخصه‌های امنیتی موجودیت فعال]، هیچکدام].

نکته کاربردی:

برای موجودیت‌ها، سرپرست مجموعه‌ای از شناسه‌ها را می‌شناسد که می‌توانند با واسط‌های مسیریاب فیزیکی مرتبط شوند؛ بنابراین این دسته از شناسه‌ها جزء شناسه‌های فرضی به حساب نمی‌آیند. اصطلاح «شناسه» به جای «آدرس» استفاده می‌شود، تا به فناوری‌هایی که مبتنی برآدرس نیستند نیز امکان مرتبط شدن با واسط مسیریاب فیزیکی را بدهند (برای مثال، شناسه مدار به جای آدرس مبدا و مقصد).

شماره **نام خانواده**

الزام

عنصر امنیتی

نویسنده هدف امنیتی باید دیگر مشخصه‌هایی که در شناسایی مجموعه موجودیت‌های مبدا و مقصد استفاده می‌شوند را، براساس فناوری پیاده‌سازی شده توسط هدف ارزیابی مشخص کند.

۶. مشخصه‌های امنیت اطلاعات

- هویت موجودیت فعال مبدا
- هویت موجودیت فعال مقصد
- پروتکل لایه انتقال
- شناسه سرویس موجودیت فعال مقصد (برای مثال، شماره پورت مقصد TCP یا UDP)

نکته کاربردی:

مفهوم « شناسه سرویس» باتوجه به پشته شبکه‌ای[1] که مورد استفاده قرار می‌گیرد ممکن است متفاوت باشد؛ منظور سرویسی است که در بالای لایه انتقال و شبکه در پشته پروتکل می‌باشد.

- [انتخاب: [اختصاص: مشخصه‌های امنیتی اطلاعات]، هیچکدام]

1 Networking stack

شماره	نام خانواده	عنصر امنیتی
الزام		

نکته کاربردی:

نویسنده هدف امنیتی، باید قسمت «اختصاص» با تمام مشخصه‌هایی که سرپرست قادر به مشخص کردن آنها در زمان ایجاد قوانین مسیریاب می‌باشد را کامل کند.

برای پشته‌های شبکه مبتنی بر غیر IP: [اختصاص: مشخصه‌های امنیتی اطلاعات]].

۱۱ **نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی معتبر) (۲)**

شماره مؤلفه: ح‌ف-ک‌ج.۲,۱(۲)((FDP_IFF.1.2(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مجوز جریان یافتن اطلاعات بین موجودیت‌های فعال مبدا و موجودیت فعال مقصد را از طریق عملیات‌های کنترل شده بدهد در صورتی‌که قوانین زیر منعقد شود:

- [موجودیت فعال مبدا، به طور موفقیت آمیز به هدف ارزیابی احراز هویت شود.
- شناسه موجودیت فعال مقصد در مجموعه‌ای از شناسه‌های مقصد باشد؛
- مشخصه‌های امنیت اطلاعات با توجه به الگوریتم‌های [اختصاص: الگوریتم‌هایی که توسط هدف ارزیابی جهت منطبق کردن

شماره **نام خانواده**

الزام

عنصر امنیتی

مشخصه‌های امنیت اطلاعات با قوانین سیاست‌گذاری اطلاعات استفاده می‌شود] منطبق بر مشخصه‌هایی در قوانین سیاست-گذاری جریان اطلاعات باشد.

- قانون سیاست‌گذاری جریان اطلاعاتی که انتخاب شده است، مجاز بودن جریان اطلاعات را مشخص کند].

نکته کاربردی:

در مسیریاب، سرپرست قوانین سیاست‌گذاری، جریان اطلاعاتی را مشخص می‌کند که حاوی مقادیر مربوط به مشخصه‌های امنیتی اطلاعات می‌باشند و با هر قانون اقدامی مرتبط شده است که یا اجازه جریان یافتن اطلاعات را می‌دهد یا جریان یافتن اطلاعات را رد می‌کند. زمانی‌که یک بسته به واسط مبدا رسید، مقادیر مشخصه‌های امنیتی اطلاعات بسته با هر یک از قوانین سیاست‌گذاری جریان اطلاعات توسط برخی از الگوریتم‌های خاص هدف ارزیابی مقایسه می‌شود و زمانی‌که یک تطابق مشاهده شد، اقدام خاص توسط آن قانون صورت می‌گیرد.

از آنجا که جایگزینی اجازه می‌دهد مشخصه‌های خاص در یک بسته، به طور بالقوه با بیش از یک قانون مطابق باشند، نویسنده هدف امنیتی نیاز دارد تا قسمت «اختصاص» را با الگوریتمی کامل گرداند که هدف ارزیابی برای یافتن قانون منطبق استفاده می‌کند.

این می‌تواند «اولین تطابق»، « خاص‌ترین تطابق» یا کمی بیش از توضیحات مفصل باشد.

شماره الزام	نام خانواده عنصر امنیتی
۱۲	**نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی معتبر) (۲)** **شماره مؤلفه: ح‌ف-ک‌ج.۱,۳(۲)((FDP_IFF.1.3(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [اختصاص: قوانین اضافی کنترل جریان اطلاعات] را اجرا کند.
۱۳	**نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی معتبر) (۲)** **شماره مؤلفه: ح‌ف-ک‌ج.۱,۴(۲)((FDP_IFF.1.4(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [سرپرست امنیتی باید پیش از بکار بردن مجموعه قوانین بتواند تمام جریان اطلاعاتی که توسط مجموعه قوانین سیاست‌گذاری جریان اطلاعات مجاز شده است را مشاهده کند] ارائه کند. **نکته کاربردی:** برخی مسیریاب‌ها قوانین بیشتری را به عنوان نتایج جانبی یک قانون ایجاد می‌نمایند؛ برای مثال، یک مسیریاب ممکن است در زمان ایجاد قانون مجاز FTP(کنترل اتصالات)، قانون مجاز کانال داده FTP را ایجاد کند. این الزام به سرپرست اجازه می‌دهد تا تمام مجموعه

شماره	نام خانواده	عنصر امنیتی
الزام		
		قوانین را مشاهده کند، به طوری‌که سرپرست می‌تواند این قوانین را شناسایی نموده و تائید کند که این مجموعه قوانین، منعکس کننده خط‌مشی مورد نظر است. منظور از عبارت «پیش از بکار بردن مجموعه قوانین» آن است که سرپرست قادر به مشاهده تمام مجموعه قوانین باشد، پیش از آنکه بر روی هدف ارزیابی قرار داده شود. این مورد به سرپرست این فرصت را می‌دهد تا هر خطا یا جریان ناخواسته را آدرس‌دهی کند.
۱۴		**نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی معتبر) (۲)** **شماره مؤلفه: ح‌ف-ک‌ج.۵,۱(۲)((FDP_IFF.1.5(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به صراحت اجازه جریان یافتن اطلاعات مبتنی بر قوانین زیر را بدهد: [هیچکدام]
۱۵		**نام عنصر: مشخصه‌های امنیتی ساده (خط‌مشی معتبر) (۲)** **شماره مؤلفه: ح‌ف-ک‌ج.۶,۱(۲)((FDP_IFF.1.6(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به صراحت جریان یافتن اطلاعات مبتنی بر قوانین زیر را انکار کند: [هیچکدام]

شماره الزام	نام خانواده	عنصر امنیتی

نکته کاربردی:

قابل ذکر است که بررسی‌های انجام شده در ح‌ف-ک‌ج.۶,۱(۱) لازم نیست که دوباره مشخص شود، زیرا این دسته از بررسی‌ها باید پیش از آنکه کاربر خود را به مسیریاب احراز هویت کند، صورت گیرد، درنتیجه آنها به جای سیاست‌گذاری معتبر بخشی از سیاست‌گذاری نامعتبر می‌باشند.

۱۶	حفاظت از اطلاعات باقیمانده (FDP_RIP)	**نام عنصر: حفاظت کامل از اطلاعات باقیمانده. ۱** **شماره مؤلفه: ح‌ف-اب.۱,۲ (FDP_RIP.2.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید این اطمینان را بدهد که هریک از مطالب اطلاعات قبلی یک منبع برای [انتخاب: تخصیص منبع به، آزادسازی منابع از] تمام موجودیت‌های غیر فعال، غیرقابل دسترس می‌باشد.

۷,۴ کلاس شناسایی و احراز هویت

توابع امنیتی هدف ارزیابی توسط سازوکارهای احتمالی و جایگشتی(همانند رمز عبور و توابع درهم‌سازی) مورد نیاز پیاده‌سازی شده‌اند (در سطح تضمین ارزیابی EAL2 به بالا).

نام کلاس: شناسایی و احراز هویت

شرح کلاس: خانواده‌های این کلاس بیان کننده الزامات مورد نیاز برای توابعی است تا بتوانند هویت کاربر ادعا شده را تصدیق و تائید نمایند. شناسایی و احراز هویت لازم و ضروری می‌باشد تا تضمین شود که کاربران دارای صفات امنیتی مناسبی می‌باشند (به طور مثال، هویت گروه‌ها، نقش‌ها، سطوح یکپارچگی یا امنیت)

شناسایی صریح کاربران مجاز و اختصاص صحیح صفات امنیتی به کاربران و موجودیت‌های فعال بسیار مهم و حساس است تا خط‌مشی‌های امنیتی در نظرگرفته شده در عمل پیاده سازی شوند. خانواده‌های این کلاس الزاماتی را فراهم می‌آورند تا هویت کاربران تعیین و احراز هویت شوند، صلاحیت آنهایی را که با هدف ارزیابی در تعامل هستند تعیین نمایند و برای هر کاربر مجاز صفات امنیتی مناسبی اختصاص داده شود. موثر اجرا شدن الزامات کلاس‌های دیگر (برای مثال، محافظت داده کاربری، ممیزی امنیتی) به شناسایی و احراز هویت صحیح کاربران بستگی دارد. این کلاس از شش خانواده تشکیل شده است که در ادامه به صورت مختصر شرح داده شده اند.

- **خانواده شکست‌ها در احراز هویت[1]**

این خانواده حاوی الزاماتی است که تعداد دفعاتی که تلاش جهت احراز هویت با شکست مواجه می‌شود را تعریف می‌کند، هم‌چنین این خانواده تعریف می‌کند که چه اقداماتی توسط توابع امنیتی هدف ارزیابی در مواردی که تلاش جهت احراز هویت با شکست مواجه می‌شود، صورت خواهد گرفت. پارامترهایی هم‌چون تعداد تلاش‌های احراز هویت منجر به شکست و آستانه زمان، در الزامات این خانواده تعیین می‌شوند.

- **خانواده تعریف مشخصه امنیتی[2]**

تمام کاربران مجاز ممکن است دارای یک مجموعه از صفات امنیتی، به غیر از هویت کاربر باشند، که در اجرای الزامات عملکرد امنیتی استفاده شده است. این خانواده الزاماتی برای مرتبط کردن صفات امنیتی کاربر به کاربران تعریف می‌کند تا در صورت لزوم توابع امنیتی هدف ارزیابی را در تصمیم‌گیری‌های امنیتی پشتیبانی کند.

- **خانواده مشخصات رازها[3]**

این خانواده تعریف کننده الزاماتی برای سازوکارهایی است که معیارهای کیفی تعریف شده را بر روی رازها اجرا می‌نمایند و هم‌چنین با توجه به همین معیارهای کیفی، رازها را تولید خواهند نمود. الزامات بر روی ساختار کلمه عبور نمونه‌ای از آن است.

1 Authentication failures(FIA_AFL)

2 User attribute definition(FIA_ATD)

3 Specification of secrets(FIA_SOS)

- **خانواده احراز هویت کاربر[1]**

این خانواده انواع سازوکارهای احراز هویت کاربر که توسط توابع امنیتی هدف ارزیابی پشتیبانی می‌شوند را تعریف می‌کند. این خانواده هم‌چنین، صفات لازمی که سازوکار احراز هویت باید بر اساس آن باشد را تعریف می‌کند.

- **خانواده شناسایی کاربر[2]**

این خانواده تعریف کننده شرایطی است که تحت آن کاربران ملزم به شناسایی خود قبل از انجام هر اقدام دیگری توسط توابع امنیتی هدف ارزیابی می‌باشند.

- **خانواده اتصال موجودیت فعال- کاربر[3]**

یک کاربر احراز هویت شده، به منظور استفاده از توابع امنیتی هدف ارزیابی معمولاً به عنوان یک موجودیت فعال در سیستم عمل می‌کند. صفات امنیتی کاربر به این موجودیت فعال نیز مرتبط می‌شود (به طور کامل یا بخشی از آن). این خانواده الزاماتی را تعریف می‌کند تا ایجاد و نگهداری ارتباط بین کاربر و موجودیت فعال متناظر با آن را فراهم آورد.

1 User authentication(FIA_UAU)

2 User identification(FIA_UID)

3 User-subject binding(FIA_USB)

شماره	نام خانواده	عنصر امنیتی
الزام		
۱۷	مدیریت رمز عبور (FIA_PMG_EXT)	**نام عنصر: مدیریت رمز عبور ۱** **شماره مؤلفه: اش-م‌ع- (ت‌س).۱,۱ (FIA_PMG_EXT.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت‌های مدیریت رمزعبور را که در زیر ذکر شده‌اند برای رمزهای عبور سرپرستی فراهم کند:

۱. رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: "@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" [,اختصاص: کاراکتر دیگر]] باشند.

۲. حداقل طول رمزعبور باید توسط سرپرست امنیت، قابل تنظیم بوده و ۱۵ کاراکتر یا بیشتر باشد.

نکته کاربردی:

نویسنده هدف امنیتی، کاراکترهای خاصی که توسط هدف ارزیابی پشتیبانی می‌شوند را انتخاب می‌کند. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» لیست کند.

«رمزعبور سرپرستی» به آن دسته از رمزعبورهایی اشاره دارد، که سرپرستان از آنها در کنسول محلی یا پروتکل‌هایی که از «رمزعبور» پشتیبانی می‌نمایند (همچون SSH,HTTPS)، استفاده می‌کنند.

شماره الزام	نام خانواده	عنصر امنیتی
۱۸	شناسایی و احراز هویت کاربر (FIA_UIA_EXT)	**نام عنصر: شناسایی و احراز هویت کاربر ۱** **شماره مؤلفه: اش-ش‌ه-(ت‌س).۱,۱ (FIA_UIA_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید پیش از آنکه به موجودیت‌های غیرهدف ارزیابی[1]، جهت شروع رویه شناسایی و احراز هویت نیاز باشد، اقدامات زیر را مجاز کند: • نمایش هشدارها مطابق با خانواده «دس_ع د.۱» • [انتخاب: بدون هیچ اقدام دیگر، [اختصاص: لیستی از سرویس‌ها، اقداماتی که توسط توابع امنیتی هدف ارزیابی جهت پاسخ دادن به در خواست‌های «غیر هدف ارزیابی» صورت می‌گیرد.]]
۱۹		**نام عنصر: شناسایی و احراز هویت کاربر ۱** **شماره مؤلفه: اش-ش‌ه-(ت‌س).۲,۱ (FIA_UIA_EXT.1.2)**

1 Non-TOE

شماره **نام خانواده**

الزام

عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید هر سرپرست را ملزم به شناسایی و احرازهویت موفق کند، پیش از آنکه به هر اقدام میانی از سوی سرپرست اجازه داده شود.

نکته کاربردی:

این الزامات به کاربران سرویس‌هایی اعمال می‌شود که از TOE به طور مستقیم قابل دسترس است و شامل سرویس‌هایی که با اتصال از طریق TOE در دسترس قرار می‌گیرند، نمی‌شود. در حالی‌که باید هیچ سرویس یا سرویس‌های کمی پیش از شناسایی و احراز هویت در دسترس موجودیت‌های خارجی باشند، در صورت وجود چنین سرویس‌هایی باید در قسمت «اختصاص» لیست شوند، در غیر این‌صورت «بدون هیچ اقدام دیگر» انتخاب می‌شود.

احراز هویت می‌تواند براساس رمز عبور از طریق یک کنسول محلی یا پروتکلی باشد که از چنین رمزهای عبوری پشتیبانی می‌کند (هم‌چون SSH)، یا براساس گواهینامه (SSH,TLS) باشد.

برای ارتباط با یک موجودیت IT خارجی (برای مثال سرور ممیزی، یا NTP سرور) چنین اتصالاتی باید مطابق با م م_ک م.۱ صورت گیرد، چنین پروتکل‌هایی شناسایی و احراز هویت را انجام می‌دهند.

شماره الزام	نام خانواده	عنصر امنیتی
۲۰	شکست‌ها در احراز هویت (FIA_AFL)	**نام عنصر: مدیریت احرازهویت ناموفق. ۱** **شماره مؤلفه: اش-ش۱.۱,۱ (FIA_AFL.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید [اختصاص: **یک عدد مثبت قابل تنظیم و غیر صفر]** از تلاش‌های ناموفق احراز هویت مربوط به [احراز هویت کاربر] را نسبت به آخرین احراز هویت موفق مشخص کنند.

نکته کاربردی:

- هدف ارزیابی ممکن است برای کاربران مختلف، روش‌های احراز هویت متفاوتی استفاده کند و از قوانین مختلفی براساس روش‌های احرازهویت/ یا کاربران جهت مدیریت کردن احراز هویت ناموفق بهره بگیرد. رفتاری که در قبال احراز هویت ناموفق، برای سیستم‌های از راه دور و کاربران انسانی صورت می‌گیرد، معمولاً متفاوت از هم می‌باشد. حتی برای کاربران انسانی ممکن است، عکس‌العمل در برابر احراز هویت ناموفق برای احراز هویتی که از طریق نام کاربری/رمزعبور صورت می‌گیرد نسبت به احراز هویتی که از طریق کارت هوشمند یا گواهینامه‌های دیجیتال انجام می‌گیرد، متفاوت باشد.

شماره	نام خانواده
الزام	

عنصر امنیتی

- رویداد احراز هویت ناموفق با توجه به آخرین نشست موفق در ترمینال شمارش می‌شود.
- هرچند که لیستی از اقدامات در برابر احراز هویت‌های ناموفق می‌تواند توسط هدف ارزیابی، مشخص شود. اما این مجموعه اقدامات باید اطمینان دهد که از حملات مبتنی بر جستجو در فضاهای ممکن جلوگیری می‌کند.

۲۱ **نام عنصر: مدیریت احرازهویت ناموفق. ۱**

شماره مؤلفه: اش-ش.ا.۲,۱.۲ (FIA_AFL.1.2)

شرح مؤلفه:

زمانی‌که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، توابع امنیتی هدف ارزیابی باید اقداماتی را که بدین منظور در نظر گرفته شده است [منع کردن کاربر از اجرای فعالیت‌هایی که مستلزم احراز هویت است تا زمانی‌که اقدامی توسط سرپرست امنیتی صورت گیرد، یا تا زمانی‌که بازه زمانی تعریف شده توسط سرپرست منقضی شود] انجام دهند.

نکته کاربردی:

از آنجا که نیازی به قفل کردن حساب کاربری سرپرست دیده نمی‌شود، این الزام برای سرپرستان محلی به کار برده نمی‌شود، بدین منظور حساب کاربری سرپرست محلی از سایر حساب‌های کاربری مجزا می‌شود، جداسازی حساب کاربری سرپرست از

شماره الزام	نام خانواده	عنصر امنیتی

کاربران می‌تواند در سند مربوط به سرپرست بیان شود یا سازوکار احراز هویت هدف ارزیابی، می‌تواند تلاش‌های ورود محلی به سیستم را از تلاش‌های ورود از راه دور به سیستم متمایز کند.

۲۲ تعریف مشخصه‌های کاربری (FIA_ATD)

نام عنصر: تعریف مشخصه‌های کاربری (هویت کاربر انسانی) ۱ (۱)

شماره مؤلفه: اش-م‌ک.۱،۱(۱) ((FIA_ATD.1.1(1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری کند:

۱. شناسه کاربر:

نقش؛

[انتخاب: [اختصاص: هر ویژگی امنیتی مربوط به شناسه کاربر(همانند گواهینامه مرتبط با شناسه کاربر)]، هیچکدام]؛ و

۲. [انتخاب: [اختصاص: دیگر ویژگی‌های امنیتی کاربر]، هیچکدام]].

نکته کاربری:

این الزام برای کاربران مجاز، سرپرستان و موجودیت‌های IT مجاز به کار برده می‌شود. با توجه به این الزام می‌توان چندین

شماره	نام خانواده	عنصر امنیتی
الزام		
		شناسه کاربری برای یک کاربر در نظر گرفت. در نتیجه اجازه داده می‌شود که برای یک کاربر انسانی نقش‌های متعددی در نظر گرفته شود، البته لازم است شناسه کاربری در ارتباط با نقش معین، احراز هویت شود. منظور از مرتبط کردن یک شناسه کاربری به یک نقش آن است که اگر نقش سرپرستی در معرض خطر قرار گیرد، میزان آسیب به حداقل برسد. اگر یک هدف ارزیابی خاص، دارای صفات مختلفی برای سرپرستان و موجودیت‌های IT مجاز باشد، انتظار می‌رود نویسنده هدف ارزیابی، این الزام را تنها یکبار برای هر مجموعه از کاربران تکرار کند تا تفاوت‌ها منعکس شود.
۲۳		**نام عنصر: تعریف مشخصه‌های کاربری** (شناسایی هدف ارزیابی به هدف ارزیابی) **۱ (۲)** **شماره مؤلفه: اش-م‌ک.۱،۱(۲) ((FIA_ATD.1.1(2))** **شرح مؤلفه:**توابع امنیتی هدف ارزیابی باید مشخصه‌های امنیتی زیر را برای هر موجودیت مجاز [1] نگهداری کند: • هویت موجودیت؛ • [اختصاص: هر ویژگی امنیتی دیگر].

1 Authorized subject

شماره الزام	نام خانواده	عنصر امنیتی
۲۴	تعریف صفات کاربر (FIA_ATD)	**نام عنصر: تعریف صفات کاربر(شناسایی هدف ارزیابی به هدف ارزیابی) ۱ (۲)** **شماره مؤلفه: اش-اه.۱,۱(۲)((2) FIA_ATD.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید لیست زیر از مشخصه‌های امنیتی متعلق به هر کاربر مجاز را نگهداری کند: • [هویت موجودیت فعال؛ [اختصاص: هر مشخصه امنیتی دیگر]].
۲۵	احراز هویت کاربر (FIA_UAU)	**نام عنصر: تعریف صفات کاربر(شناسایی هدف ارزیابی به هدف ارزیابی) ۱ (۲)** **شماره مؤلفه: اش-اه.۱,۲(۲)((2) FIA_UAU.2.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت احراز هویت کند.
۲۶		**نام عنصر: سازوکار احراز هویت مبتنی بر رمزعبور ۲**

شماره الزام	نام خانواده عنصر امنیتی
	شماره مؤلفه: اش-اه.(ت‌س).۱,۲ (FIA_UAU_(EXT).2.1)
	شرح مؤلفه:
	توابع امنیتی هدف ارزیابی جهت احراز هویت سرپرستان باید یک سازوکار احراز هویت محلی مبتنی بر رمز عبور[انتخاب:[اختصاص: دیگر سازوکارهای احراز هویت]، هیچکدام] را فراهم کند.
۲۷	**نام عنصر: احراز هویت کاربر ۵**
	شماره مؤلفه: اش-اه.(ت‌س).۱,۵ (FIA_UAU_(EXT).5.1)
	شرح مؤلفه:
	توابع امنیتی هدف ارزیابی، باید سازوکار احراز هویت محلی، [انتخاب:[اختصاص: دیگر سازوکارهای احراز هویت]، هیچکدام] ارائه کند، تا کاربر را احراز هویت کند.
	نکته کاربردی:
	این الزام توسعه یافته از آن جهت لازم و ضروری است که در استاندارد معیار مشترک، هیچ الزام دیگری که توابع امنیتی هدف ارزیابی را ملزم به ارائه احراز هویت کند، وجود ندارد. (این الزام به طور ضمنی توسط دیگر الزامات خانواده اش-اه به کار برده شده است).

شماره	نام خانواده	عنصر امنیتی
الزام		
		نویسنده هدف امنیتی، می‌تواند در قسمت انتخاب، مورد اول را انتخاب کند در این صورت قسمت «اختصاص» را با هر سازوکار احراز هویت، می‌تواند کامل کند، همانند سازوکاری که کاربران را با استفاده از گواهینامه، احراز هویت می‌کند. در صورت انتخاب الگوریتم نامتقارن، هدف ارزیابی ممکن است با تکیه بر سرور احراز گواهینامه، گواهینامه کاربر را به دست آورد و این سرور را به عنوان یک موجودیت IT مجاز در نظر بگیرد در این صورت الزامات محیط IT باید بر روی این موجودیت IT نیز اعمال شود.
۲۸		**نام عنصر: احراز هویت کاربر ۷**
		شماره مؤلفه: اش-اه.(ت‌س).۱,۷ (FIA_UAU_(EXT).7.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید زمانی‌که فرآیند احراز هویت، در کنسول محلی در حال صورت گرفتن است؛ تنها باید به سرپرست، بازخورد مبهمی[1] ارائه دهند.
		نکته کاربردی:
		«بازخورد مبهم» نشان می‌دهد که توابع امنیتی هدف ارزیابی نمایش واضحی از هر داده‌ای که جهت احراز هویت شدن توسط

1 Obscured feedback

شماره	نام خانواده	عنصر امنیتی
الزام		
		کاربر وارد می‌شود، ندارد (مانند انعکاس رمز عبور). هر چند «بازخورد مبهمی» از روند احراز هویت ممکن است ارائه شود (همچون * که در زمان وارد کردن هر کاراکتر توسط کاربر، نشان داده می‌شود). «بازخورد مبهم» همچنین نشان می‌دهد که توابع امنیتی هدف ارزیابی، هیچ اطلاعاتی را در طول رویه احراز هویت به کاربر برنمی‌گرداند.
۲۹	شناسایی کاربر (FIA_UID)	**نام عنصر:** شناسایی کاربر پیش از هر اقدامی **۲** **شماره مؤلفه: اش-ش‌ک.۱,۲ (FIA_UID.2.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت شناسایی کند.
۳۰	اتصال موجودیت‌های فعال کاربر (FIA_USB)	**نام عنصر: اتصال موجودیت‌های فعال کاربر ۱** **شماره مؤلفه: اش-م‌ف.۱,۱ (FIA_USB.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید صفات امنیتی کاربر که در ادامه مطرح شده است را به موجودیت‌های فعال از سوی آن کاربر مرتبط

شماره الزام	نام خانواده	عنصر امنیتی
		کند: [اختصاص: لیستی از صفات امنیتی کاربر].
۳۱		**نام عنصر: اتصال موجودیت‌های فعال کاربر ۱** **شماره مؤلفه: اش-م‌ف.۲,۱ (FIA_USB.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید قوانین زیر را بر روی پیوند اولیه صفات امنیتی کاربر به موجودیت فعالی که از سوی کاربر عمل می‌کند، اجرا کند. [اختصاص: قوانینی برای ارتباط اولیه مشخصه‌ها]
۳۲		**نام عنصر: اتصال موجودیت‌های فعال کاربر ۱** **شماره مؤلفه: اش-م‌ف.۳,۱ (FIA_USB.1.3)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قوانین زیر را که ناظر بر تغییرات مشخصه‌های امنیتی کاربر مرتبط با موجودیت‌های فعال از سوی کاربر است را اجرا کند:

شماره	نام خانواده	عنصر امنیتی
الزام		

[اختصاص: قوانینی برای تغییر مشخصه‌های امنیتی]

۷,۵ کلاس مدیریت امنیت

در ادامه المان‌های امنیتی مورد نیاز کلاس مدیریت امنیت ارائه شده است.

نام کلاس: مدیریت امنیت

شرح کلاس: این کلاس جهت مشخص کردن مدیریت ویژگی‌های مختلف توابع امنیتی هدف ارزیابی در نظر گرفته شده است: ویژگی‌های امنیتی، توابع و داده‌های توابع امنیتی هدف ارزیابی.

هم‌چنین در این کلاس نقش‌های مدیریتی مختلف و تعاملاتشان، هم‌چون جداسازی قابلیت‌ها می‌تواند مشخص شود. این کلاس دارای چندین هدف است:

- مدیریت داده توابع امنیتی هدف ارزیابی، برای مثال علامت‌ها[1]
- مدیریت صفات امنیتی، برای مثال لیست‌های کنترل دسترسی و لیست قابلیت‌ها
- مدیریت عملکرد توابع امنیتی هدف ارزیابی برای مثال، انتخاب توابع ، نقش‌ها یا شرایطی که رفتار توابع امنیتی هدف ارزیابی را تحت تاثیر قرار می‌دهند.
- تعریف نقش‌های امنیتی

شرح مختصری از خانواده‌های این کلاس در ادامه آمده است.

- **خانواده مدیریت کارکردها در توابع امنیتی هدف ارزیابی[1]**

1 Banner

این خانواده اجازه می‌دهد کنترل کاربران مجاز در حین مدیریت کارکرد توابع امنیتی هدف ارزیابی انجام شود. مثالی از عملکردها در توابع امنیتی هدف ارزیابی، شامل ممیزی توابع و توابع احراز هویت چندگانه می‌باشد.

- **خانواده مدیریت مشخصات امنیتی[۲]**

این خانواده اجازه می‌دهد کنترل کاربران مجاز طی مدیریت مشخصات امنیتی انجام شود. این مدیریت می‌تواند شامل قابلیتی برای مشاهده و تغییر مشخصات امنیتی باشد.

- **خانواده مدیریت داده‌های توابع امنیتی هدف ارزیابی[۳]**

این خانواده اجازه کنترل کاربران (نقش‌های) مجاز را طی مدیریت داده‌های توابع امنیتی هدف ارزیابی می‌دهد. مثالی از داده توابع امنیتی هدف ارزیابی می‌تواند شامل ممیزی اطلاعات، ساعت و دیگر پارامترهای پیکربندی توابع امنیتی هدف ارزیابی باشد.

- **خانواده لغو[۴]**

این خانواده نشان دهنده لغو مشخصات (صفات) امنیتی انواع موجودیت‌ها در داخل هدف ارزیابی می‌باشد.

- **خانواده انقضای ویژگی‌های امنیتی[۵]**

این خانواده قادر به اعمال محدودیت زمانی بر روی اعتبار مشخصات(صفات) امنیتی می‌باشد.

---

1 Management of functions in TSF(FMT_MOF)
2 Management of security attributes(FMT_MSA)
3 Management of TSF data(FMT_MTD)
4 Revocation(FMT_REV)
5 Security attribute expiration(FMT_SAE)

➢ خانواده مشخصات کارکردهای مدیریتی[1]

این خانواده اجازه می‌دهد تا مشخصات کارکردهای مدیریتی توسط هدف ارزیابی ایجاد شوند. کارکردهای مدیریتی با استفاده از ایجاد رابط توابع امنیتی هدف ارزیابی، به سرپرستان اجازه می‌دهند تا پارامترهایی برای کنترل عملکرد ویژگی‌های مربوط به امنیت هدف ارزیابی را تعریف نمایند، مانند مجوزها و صفات حفاظت از داده، مجوزها و صفات حفاظت از هدف ارزیابی، مجوزها و صفات ممیزی و مجوزها و صفات شناسایی و احراز هویت.

کارکردهای مدیریتی هم‌چنین شامل آن دسته از کارکردهایی است که توسط کاربر اجرا می‌شود تا تداوم کارکرد هدف ارزیابی را تضمین کند، مانند کارکردهای پشتیبانی و بازیابی. کارکرد این خانواده بر روی دیگر مؤلفه‌ها در کلاس مدیریت امنیت تاثیر دارد.

➢ خانواده نقش‌های مدیریت امنیتی[2]

این خانواده برای کنترل اختصاص نقش‌های مختلف به کاربران در نظرگرفته شده است. توانایی این نقش‌ها با توجه به مدیریت امنیتی است که در دیگر خانواده‌های این کلاس توصیف شده است.

شماره الزام	نام خانواده	عنصر امنیتی
۳۳		**نام عنصر: مدیریت داده های توابع امنیتی هدف ارزیابی ۱**
	مدیریت داده های	

1 Specification of Management Functions (FMT_SMF)

2 Security management roles (FMT_SMR)

شماره الزام	نام خانواده	عنصر امنیتی
	توابع امنیتی هدف ارزیابی (FMT_MTD)	**شماره مؤلفه: م‌د-م‌د.۱،۱(FMT_MTD.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید توانایی مدیریت داده‌های توابع امنیتی هدف ارزیابی را تنها به سرپرست امنیتی محدود کند. **نکته کاربردی:** عبارت «**مدیریت**» می‌تواند شامل انجام موارد زیر باشد، اما تنها به این موارد نیز محدود نمی‌شود: • ایجاد، مقداردهی، مشاهده، تغییر پیش‌فرض، تغییردادن،-حذف کردن، پاک کردن و اضافه کردن این الزام به طور پیش‌فرض برای مدیریت داده توابع امنیتی هدف ارزیابی درنظرگرفته می‌شود. به عنوان مثال داده‌های توابع امنیتی هدف ارزیابی می‌تواند شامل اطلاعات رمزنگاری باشد و هم‌چنین مدیریت این داده‌ها شامل مرتبط کردن یک پروتکل رمزنگاری به یک واسط می‌باشد.
۳۴	مشخصات عملکردهای مدیریتی (FMT_SMF)	**نام عنصر: مشخصات عملکردهای مدیریتی ۱** **شماره مؤلفه: م‌د-ع‌م.۱،۱(FMT_SMF.1.1)** **شرح مؤلفه:**

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید توانایی اجرای عملکردهای مدیریتی زیر را داشته باشد:

- توانایی سرپرستی کردن هدف ارزیابی به صورت محلی و از راه دور
- توانایی به روزرسانی هدف ارزیابی و تائید صحت به روزرسانی با استفاده از روش [انتخاب: امضای دیجیتال، کد درهم‌سازی منتشر شده، بدون سازوکار دیگر] پیش از آنکه به‌روزرسانی نصب شود.
- [انتخاب:
  - توانایی پیکربندی لیستی از سرویس‌های در دسترس ارائه شده توسط هدف ارزیابی، پیش از آنکه یک موجودیت به صورت مشخص شده در اش-ش ه-(ت س).۱ شناسایی و احراز هویت شود.
  - توانایی پیکربندی توابع رمزنگاری
  - بدون هیچ قابلیت دیگری]

نکته کاربردی:

هدف ارزیابی باید ارائه دهنده عملکردی برای سرپرستی از راه دور و محلی باشد، هم‌چنین باید امکانی را برای سرپرستان فراهم کند تا بتوانند به روزرسانی‌های دریافت شده از منبع امن را تائید نمایند. سرپرست باید بتواند این‌گونه اقدامات را با استفاده از

شماره الزام	نام خانواده	عنصر امنیتی
		امضای دیجیتال و کد درهم‌سازی منتشر شده، انجام دهد. نویسنده هدف امنیتی، در اولین «انتخاب» باید مشخص کند به روزرسانی‌ها چگونه تائید می‌شوند، هر انتخاب در این قسمت باید با انتخاب در الزام «حت-رم-(ت‌س)» مطابقت داشته باشد. چنان‌چه هدف ارزیابی این توانائی را به سرپرست بدهد تا سرویس‌های در دسترس را پیش از شناسایی و احراز هویت پیکربندی کند، یا اگر هر عملکرد رمزنگاری بر روی هدف ارزیابی بتواند پیکربندی شود، بنابراین نویسنده هدف امنیتی مورد مناسب را انتخاب می‌کند، یا در دومین انتخاب، عبارت «بدون هیچ قابلیت دیگری» را انتخاب می‌کند.
۳۵		**نام عنصر: محدودسازی نقش‌های امنیتی ۲** **شماره مؤلفه: مد-ن‌م.۲,۱(FMT_SMR.2.1)** **شرح مؤلفه:**
	نقشهای امنیتی (FMT_SMR)	توابع امنیتی هدف ارزیابی، باید نقش‌های زیر را نگهداری کنند: • سرپرست مجاز
۳۶		**نام عنصر: محدودسازی نقش‌های امنیتی ۲** **شماره مؤلفه: مد-ن‌م.۲,۲(FMT_SMR.2.2)**

شماره الزام	نام خانواده	عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به مرتبط کردن کاربران با نقش‌هایشان باشد.

نکته کاربردی:

لازم است حساب‌های کاربری تنها با یک نقش مرتبط شده باشند. هرچند ممکن است چندین کاربر نقش مشابهی داشته باشند و نیازی نیست که هدف ارزیابی نقش‌ها را تنها به یک کاربر محدود کند.

۳۷ **نام عنصر: محدودسازی نقش‌های امنیتی ۲**

شماره مؤلفه: م‌د-ن‌م.۳,۲(FMT_SMR.2.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید تضمین کند که شرایط زیر برآورده می‌شوند:

- نقش سرپرست مجاز که باید قادر به سرپرستی هدف ارزیابی به صورت محلی باشد.
- نقش سرپرست مجاز که باید قادر به سرپرستی هدف ارزیابی به صورت از راه دور باشد.

نکته کاربردی :

شماره الزام	نام خانواده	عنصر امنیتی
		لازم است که سرپرست مجاز قادر به سرپرستی هدف ارزیابی از طریق کنسول محلی یا سازوکارهای راه دور (IPsec, SSH, TLS, TLS/HTTPS) باشد. برای هدف ارزیابی دارای چندین مؤلفه، تنها مؤلفه‌های هدف ارزیابی که ارائه دهنده کنترل مدیریت و پیکربندی دیگر مؤلفه هدف ارزیابی باشند، نیاز به یک واسط اجرایی محلی[1] دارند.
۳۸	مدیریت توابع در توابع امنیتی هدف ارزیابی (FMT_MOF)	**نام عنصر: مدیریت رفتار توابع امنیتی (خودآزمایی توابع امنیتی هدف ارزیابی به غیر از رمزنگاری) ۱(۱)** **شماره مؤلفه: مد-مت.۱,۱(۱)(۱)(FMT_MOF.1.1(1))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت تغییر رفتار توابع [خودآزمایی توابع امنیتی هدف ارزیابی (حت-خا-(تس).۱)] به [سرپرست امنیتی] محدود کند. **نکته کاربردی:** «تغییر رفتار» اشاره به مشخص کردن بازه‌ای است که آزمون یا یک زیرمجموعه از آزمون‌های منتخب به طور متناوب اجرا می‌شوند.

1 Local administration interface

شماره الزام	نام خانواده	عنصر امنیتی
۳۹		**نام عنصر: مدیریت رفتار توابع امنیتی (خودآزمایی رمزنگاری) ۱(۲)**
		شماره مؤلفه: مد-مت.۱٫۱(۲)(FMT_MOF.1.1(2))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیت فعال کردن و غیرفعال کردن توابع
		[خودآزمایی توابع امنیتی هدف ارزیابی حت-خا-.۱(۱) و حت-خا-.۱(۲)] به
		[سرپرست رمزنگاری] محدود کند.
		نکته کاربردی:
		فعال‌سازی و غیرفعال کردن آزمون خودآزمایی رمزنگاری بلافاصله پس از تولید کلید صورت می‌گیرد.
۴۰		**نام عنصر: مدیریت رفتار توابع امنیتی (بازبینی ممیزی) ۱(۳)**
		شماره مؤلفه: مد-مت.۱٫۱(۳)(FMT_MOF.1.1(3))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیت فعال کردن، غیرفعال کردن، تعیین و تغییر رفتار توابع

شماره الزام	نام خانواده	عنصر امنیتی
		[ممیزی امنیت (ما-ب‌ز.۱، ما-ب‌ز.۲، ما-ب‌ز.۳)] به
		[سرپرست ممیزی] محدود کند.
۴۱		**نام عنصر: مدیریت رفتار توابع امنیتی (انتخاب ممیزی) ۱(۴)**
		شماره مؤلفه: مد-مت.۱٫۱(۴)(FMT_MOF.1.1(4))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیت فعال کردن، غیرفعال کردن، تعیین و تغییر رفتار توابع
		[آنالیز ممیزی امنیت (ما-ت‌ح)؛ و
		ممیزی امنیت(ما-اخ)] به
		[سرپرست امنیتی] محدود کند.
		نکته کاربردی:
		برای توابع ممیزی، فعال و غیر فعال سازی اشاره به فعال کردن و غیر فعال کردن سازوکارهای ممیزی دارد.
		«تعیین رفتار» به معنی توانایی تعیین کردن صریح آنچه که بر روی سیستم ممیزی گردیده است، می‌باشد. در حالی‌که «تغییر رفتار» به

شماره الزام	نام خانواده	عنصر امنیتی

معنی تنظیم کردن یا نکردن ویژگی‌های خاصی از سازوکارهای ممیزی است.

۴۲ **نام عنصر: مدیریت رفتار توابع امنیتی (هشدارها) ۱(۵)**

شماره مؤلفه: مد-مت.۱,۱(۵)(FMT_MOF.1.1(5))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت فعال کردن، غیرفعال کردن توابع

[هشدارهای امنیتی (ما-پس)] به

[سرپرست امنیتی] محدود کند.

نکته کاربردی:

این الزام تضمین می‌کند که تنها سرپرستان امنیتی می‌توانند عملکرد اعلام هشدار را فعال یا غیر فعال (خاموش یا روشن) نمایند. همان-طور که در این قسمت گفته شده است، نمی‌توان رفتار ما-پس.۱ را تغییر داد. در صورتی‌که نویسنده هدف امنیتی در برگیرنده عملکرد بیشتری در ما-پس.۱باشد، آنگاه نویسنده هدف امنیتی باید «تغییر رفتار» را نیز برای این الزام در نظر بگیرد.

۴۳ **نام عنصر: مدیریت رفتار توابع امنیتی (سازوکار ظرفیت) ۱(۶)**

شماره الزام	نام خانواده	عنصر امنیتی

شماره مؤلفه: مد-مت.۱٫۱(۶)(FMT_MOF.1.1(6))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت تعیین رفتار توابع

- [تخصیص منابع اتصال‌گرای کنترل شده (من-تم)؛
- شناسه شبکه یک سرپرست مشخص؛
- تنظیم کردن شناسه شبکه یک سرپرست خاص؛
- دوره زمانی یک سرپرست مشخص] به

[سرپرست امنیتی] محدود کند.

نکته کاربردی:

«تعیین رفتار» به مشخص کردن شناسه شبکه‌ای اشاره دارد که با استفاده از الزام من-تم.۱(۲) پیگیری می‌شود و بازه زمانی که بر روی محدودسازی ظرفیت به اجرا در می‌آید.

۴۴ **نام عنصر: مدیریت رفتار توابع امنیتی (تلاش‌های احرازهویت) ۱(۷)**

شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: مد-مت.۱,۱(۷)(FMT_MOF.1.1(7))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیت فعال‌سازی، غیر فعال‌سازی، تعیین و تغییر رفتار توابع
		[اداره شکست احراز هویت (اش-ش.۱,۲)، **تنظیم یک عدد مثبت و غیر صفر** از تلاش‌های ناموفق احراز هویت مربوط به احراز هویت
		کاربر را] به [سرپرست امنیتی] محدود کند.
۴۵		**نام عنصر: مدیریت مشخصه‌های امنیتی (نامعتبر) ۱ (۱)**
		شماره مؤلفه: مد-م.۱,۱(۱) (FMT_MSA.1.1(1))
		شرح مؤلفه:
	مدیریت مشخصه‌های امنیتی **(FMT_MSA)**	توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعاتی نامعتبر] اجرا کند، تا قابلیت [انتخاب: تغییر-پیش‌فرض، پرس‌وجو، تغییر دادن، حذف کردن، [اختصاص: دیگر عملیات‌ها]] مشخصه‌های امنیتی [درصد قابل تنظیم ظرفیت ذخیره‌سازی، [اختصاص: لیستی از مشخصه‌های امنیتی]] به [سرپرست امنیتی، [نقش‌های معرفی‌شده مجاز]] محدود کند.
۴۶		**نام عنصر: مدیریت مشخصه‌های امنیتی (معتبر) ۱ (۲)**

شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: م‌د-م‌ا.۱,۱(۲) (FMT_MSA.1.1(2))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعاتی معتبر] اجرا کند، تا قابلیت [انتخاب: تغییر-پیش‌فرض، پرس-وجو، تغییر دادن، حذف کردن، [اختصاص: دیگر عملیات‌ها]] مشخصه‌های امنیتی [درصد قابل تنظیم ظرفیت ذخیره‌سازی، [اختصاص: لیستی از مشخصه‌های امنیتی]] به [سرپرست امنیتی، [نقش‌های معرفی‌شده مجاز]] محدود کند.
۴۷		**نام عنصر: صفات امنیتی امن ۲**
		شماره مؤلفه: م‌د-م‌ا.۱,۲ (FMT_MSA.2.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید این اطمینان را بدهد که تنها مقادیر امن برای صفات امنیتی پذیرفته می‌شود.
۴۸		**نام عنصر: صفات امنیتی امن ۳ (۱)**
		شماره مؤلفه: م‌د-م‌ا.۱,۳ (۱) (FMT_MSA.3.1(1))
		شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعاتی نامعتبر] اجرا کند، تا مقادیر پیش‌فرض محدودی برای مشخصه‌های امنیتی که در اجرای خط‌مشی‌های عملکرد امنیتی استفاده می‌شوند، فراهم کند.

نکته کاربردی:

«محدود» در این‌جا به این معنی است که با اطلاعات پیش‌فرض اجازه جاری شدن داده نمی‌شود (باتوجه به خط‌مشی‌های اشاره شده) مگر آنکه یک مشخصه اجرایی صریح، اجازه جریان یافتن اطلاعات را بدهد.

۴۹ **نام عنصر: صفات امنیتی امن ۳ (۱)**

شماره مؤلفه: م‌د-م‌ا.۲,۳ (۱) (FMT_MSA.3.2(1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به [سرپرست امنیتی] اجازه دهد تا مقادیر اولیه جایگزین را مشخص کند تا مقادیر پیش‌فرض را در زمان ایجاد یک اطلاعات یا رویداد، نادیده بگیرد.

۵۰ **نام عنصر: صفات امنیتی امن ۳ (۲)**

شماره مؤلفه: م‌د-م‌ا.۱,۳ (۲) (FMT_MSA.3.1(2))

شماره الزام	نام خانواده	عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [خط‌مشی عملکرد امنیتی جریان اطلاعاتی معتبر] اجرا کند، تا مقادیر پیش‌فرض محدودی برای مشخصه-های امنیتی که در اجرای خط‌مشی‌های عملکرد امنیتی استفاده می‌شوند، فراهم کند.

نکته کاربردی:

«محدود» در این‌جا به این معنی است که با اطلاعات پیش‌فرض اجازه جاری شدن داده نمی‌شود (باتوجه به خط‌مشی‌های اشاره شده) مگر آنکه یک مشخصه اجرایی صریح، اجازه جریان یافتن اطلاعات را بدهد، به طور پیش‌فرض اطلاعات، مجاز به جاری شدن نمی‌باشد.

۵۱ **نام عنصر: صفات امنیتی امن ۳ (۲)**

شماره مؤلفه: م‌د-م‌ا.۲,۳.۲ (۲) (FMT_MSA.3.2(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به [سرپرست امنیتی] اجازه دهد تا مقادیر اولیه جایگزین را مشخص کند تا مقادیر پیش‌فرض را در زمان ایجاد یک اطلاعات یا رویداد، نادیده بگیرد.

۵۲ مدیریت داده‌های **نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی(غیر رمزنگاری، داده توابع امنیتی هدف ارزیابی غیر زمانی) ۱ (۱)**

شماره الزام	نام خانواده	عنصر امنیتی
	توابع امنیتی هدف ارزیابی (FMT_MTD)	**شماره مؤلفه: مد-مد.۱،۱(۱) ((FMT_MTD.1.1(1))**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید قابلیت [انتخاب: تغییر-پیش‌فرض، پرس‌وجو، تغییر دادن، حذف کردن، پاک کردن [انتخاب: [اختصاص: دیگر عملیات‌ها]، هیچکدام]] تمام [داده‌های توابع امنیتی هدف ارزیابی به جز داده‌های تضمین رمزنگاری و زمان و تاریخی که به صورت مهرهای زمانی در ح‌ت-م‌ز.۱ استفاده می‌شود] را به [سرپرست‌های موجودیت‌های IT مجاز] محدود کند.

نکته کاربردی:

نویسنده هدف امنیتی باید در صورت لزوم این الزام را تکرار کند تا این اطمینان را بدهد که داده توابع امنیتی هدف ارزیابی به صورت قابلیت ارائه شده توسط هدف ارزیابی، مشخص شده است و آنکه دسترسی مناسب تنها به سرپرستان شایسته و موجودیت‌های IT مجاز محدود شده است.

داده تضمین رمزنگاری و داده مهرهای زمانی در دو مؤلفه زیر پوشش داده شده است که دارای الزامات خاص برای آدرس دهی پروفایل-های حفاظتی تهدیدها و خط‌مشی‌ها هستند.

۵۳ **نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی (داده توابع امنیتی هدف ارزیابی رمزنگاری) ۱ (۲)**

شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: مد-مد.۱٫۱(۲) ((FMT_MTD.1.1(2))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید قابلیت تغییر دادن [داده امنیت رمزنگاری] به [سرپرست رمزنگاری] محدود کند.
		نکته کاربردی:
		منظور این الزام محدود کردن توانایی پیکربندی خط‌مشی رمزنگاری هدف ارزیابی به سرپرست رمزنگاری می‌باشد. پیکربندی خط‌مشی رمزنگاری با چیزهایی هم‌چون تنظیم مود عملیاتی، دوره کلید، انتخاب یک الگوریتم خاص و اندازه طول کلید مرتبط است.
۵۴		**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی (داده توابع امنیتی هدف ارزیابی زمانی) ۱ (۳)**
		شماره مؤلفه: مد-مد.۱٫۱(۳) ((FMT_MTD.1.1(3))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید قابلیت [تنظیم کردن] [زمان و تاریخی که به صورت مهرهای زمانی در حت-مز.۱ استفاده می‌شود] را به [سرپرست‌های موجودیت‌های IT مجاز] محدود کند.
		نکته کاربردی:

شماره الزام	نام خانواده	عنصر امنیتی

نویسنده هدف امنیتی، قادر است قابلیت تنظیم زمان و تاریخ را تنها به سرپرستان امنیتی یا تنها به موجودیت‌های IT مجاز یا هر دو محدود کند.

۵۵ **نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی(مجموعه قوانین خط‌مشی جریان اطلاعات) ۱ (۴)**

شماره مؤلفه: م‌د-م‌د.۱،۱(۴) (FMT_MTD.1.1(4))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید قابلیت پرس‌وجو، تغییر دادن، حذف کردن، ایجاد[انتخاب: [اختصاص: دیگر عملیات‌ها]، هیچکدام] [قوانین خط‌مشی جریان اطلاعات] را به [سرپرست‌های امنیتی] محدود کند.

نکته کاربردی:

این الزام مشخصات مجموعه قوانین خط‌مشی جریان اطلاعات را که در ح‌ف-ک‌ج معرفی شده است را به سرپرست امنیتی محدود می‌کند. نویسنده هدف امنیتی باید هر عملیات خاص هدف ارزیابی را که سرپرست می‌تواند بر روی مجموعه قوانین انجام دهد در قسمت «اختصاص» عنوان کند.

۵۶ **نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی (ظرفیت لایه انتقال) ۲ (۱)**

شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: مد-مد.۱,۲(۱) (FMT_MTD.2.1(1))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید تعیین محدوده برای [ظرفیت بر روی اتصالات لایه انتقال] را به [سرپرست‌های امنیتی] محدود کند.
۵۷		**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی (ظرفیت لایه انتقال) ۲ (۱)**
		شماره مؤلفه: مد-مد.۲,۲(۱) (FMT_MTD.2.2(1))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید اقدامات[اختصاص: اقدامات] انجام دهد، چنان‌چه داده توابع امنیتی هدف ارزیابی از حدود مشخصی تجاوز کند.
		نکته کاربردی:
		قابل توجه است که در الزام من-ت‌م.۱(۱)، نشان داده نمی‌شود که هدف ارزیابی باید سرپرست امنیتی با قابلیت تنظیم حداکثر را ارائه کند، اگر چه هدف ارزیابی چنین سازوکاری را ارائه دهد، بنابراین الزام مد-مد.۱,۲(۱) ملزم می‌کند که این سازوکار تنها به سرپرست امنیتی محدود شود.

شماره الزام	نام خانواده	عنصر امنیتی
		برای مد-مد.۲,۲(۱)، نویسنده هدف امنیتی باید اقداماتی را مشخص کند تا در زمانی‌که ظرفیت به حد معینی رسید ، صورت بگیرد.
۵۸		**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی(ظرفیت اتصال‌گرای کنترل شده) ۲ (۲)** **شماره مؤلفه: مد-مد.۱,۲(۲) (FMT_MTD.2.1(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید تعیین محدوده برای [ظرفیت منابع اتصال‌گرای کنترل شده] را به [سرپرست‌های امنیتی] محدود کند.
۵۹		**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی(ظرفیت اتصال‌گرای کنترل شده) ۲ (۲)** **شماره مؤلفه: مد-مد.۲,۲(۲) (FMT_MTD.2.2(2))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید اقدامات[اختصاص: اقدامات] انجام دهد، چنان‌چه داده توابع امنیتی هدف ارزیابی از حدود مشخصی تجاوز کند. **نکته کاربردی:** برای مد-مد.۲,۲(۲)، نویسنده هدف امنیتی باید مشخص کند که چه اقداماتی باید برای هر منبع اتصال گرای کنترل شده صورت بگیرد،

شماره الزام	نام خانواده	عنصر امنیتی
		در زمانی‌که ظرفیت تعیین شده توسط سرپرست امنیتی حاصل می‌شود.
		این الزام ممکن است با توجه به من-ت‌م.۱(۲) تکرار شود. جهت جزئیات بیشتر این الزام برای سازوکار ظرفیت به نکته کاربردی من-ت‌م.۱ (۲) توجه شود.
۶۰		**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی(درصد ظرفیت ذخیره‌سازی) ۲ (۳)**
		شماره مؤلفه: م‌د-م‌د.۱,۲(۳) (FMT_MTD.2.1(3))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید تعیین محدوده برای [ظرفیت منابع اتصال‌گرای کنترل شده] را به [سرپرست‌های امنیتی] محدود کند.
۶۱		**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی (درصد ظرفیت ذخیره‌سازی) ۲ (۳)**
		شماره مؤلفه: م‌د-م‌د.۲,۲(۳) (FMT_MTD.2.2(3))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید اقدامات [اختصاص: اقدامات] انجام دهد، چنان‌چه داده توابع امنیتی هدف ارزیابی از حدود مشخصی تجاوز کند.

شماره الزام	نام خانواده	عنصر امنیتی
		نکته کاربردی:
		برای مد-م‌د.۲,۲(۱)، نویسنده هدف ارزیابی، باید اقداماتی را که هدف ارزیابی در زمان رسیدن به درصد تعیین شده، انجام می‌دهد را مشخص کند.
		این اختصاص باید با انتخاب/اختصاص انجام شده در FAU_STG.NIAP-0414-1.1-NIAP-0429 سازگاری داشته باشد.
۶۲		**نام عنصر: لغو ۱**
		شماره مؤلفه: م‌د-ل‌غ.۱,۱(FMT_REV.1.1)
		شرح مؤلفه:
	لغو (FMT_REV)	توابع امنیتی هدف ارزیابی، باید قابلیت لغو مشخصه‌های امنیتی مرتبط با [انتخاب: کاربران، موجودیت فعال، موجودیت غیرفعال، [اختصاص: دیگر منابع اضافی]] در داخل TSC را به [سرپرست امنیتی] محدود کند.
۶۳		**نام عنصر: لغو ۱**
		شماره مؤلفه: م‌د-ل‌غ.۲,۱(FMT_REV.1.2)
		شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی
		توابع امنیتی هدف ارزیابی، باید قوانین زیر را اجرا کند: [اختصاص: مشخص کردن قوانین لغو]
۶۴		**نام عنصر: مشخصات عملکردهای مدیریتی ۱**
		شماره مؤلفه: م‌د-ع‌م.۱،۱،۱(FMT_SMF.1.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید قادر به انجام عملکرد مدیریت امنیتی زیر باشد:
	مشخصات عملکردهای مدیریتی **(FMT_SMF)**	۱. محدود کردن قابلیت اتخاذ تصمیم و تغییر رفتار عملکرد خودآزمایی توابع امنیتی هدف ارزیابی (ح‌ت-خا-(ت‌س).۱) به سرپرست امنیتی ۲. محدود کردن قابلیت فعال کردن و غیر فعال کردن عملکرد خودآزمایی توابع امنیتی هدف ارزیابی (ح‌ت-خا.۱(۱) و ح‌ت-خا.۱(۲)) به سرپرست رمزنگاری ۳. محدود کردن قابلیت فعال کردن، غیر فعال کردن، تعیین و تغییر رفتار عملکرد تحلیل ممیزی امنیت (م‌ا-ب‌ز.۱ ، م‌ا-ب‌ز.۲ و م‌ا-ب‌ز.۳) به سرپرست ممیزی ۴. محدود کردن قابلیت فعال کردن، غیر فعال کردن، تعیین و تغییر رفتار عملکرد تحلیل ممیزی امنیت (م‌ا-ت‌ح)؛ و ممیزی امنیت

شماره الزام	نام خانواده	عنصر امنیتی

به (ما-اخ) سرپرست امنیتی

۵. محدود کردن قابلیت فعال کردن، غیر فعال کردن عملکرد هشدار امنیتی (ما-پ‌س) به سرپرست امنیتی

۶. محدود کردن قابلیت تعیین رفتار عملکردهای زیر به سرپرست:

- اختصاص منابع اتصال‌گرای کنترل شده (من-ت‌م.۱(۲))
- شناسه شبکه مختص سرپرست
- تنظیم شناسه شبکه مختص سرپرست
- بازه زمانی مختص سرپرست

۷. به اجرا گذاردن حداکثر ظرفیت مختص سرپرست از منابع زیر: [منابع اتصال‌گرای کنترل شده] که کاربران در ارتباط با [شناسه شبکه مختص سرپرست و تنظیم شناسه شبکه مختص سرپرست] می‌توانند بر روی یک بازه زمانی مختص سرپرست استفاده شوند.

۸. اجرای [خط‌مشی‌های عملکرد امنیتی جریان اطلاعات نامعتبر] تا مقادیر پیش‌فرض مشخصه‌های امنیتی که برای اجرای خط-مشی‌های عملکرد امنیتی استفاده می‌شوند را محدود کند.

شماره الزام	نام خانواده	عنصر امنیتی

۹. اجرای [خط‌مشی‌های عملکرد امنیتی جریان اطلاعات معتبر] تا مقادیر پیش‌فرض مشخصه‌های امنیتی که برای اجرای خط‌مشی-های عملکرد امنیتی استفاده می‌شوند را محدود کند.

۱۰. محدود کردن قابلیت [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر دادن، حذف کردن، پاک کردن، [انتخاب: [اختصاص: دیگر عملیات‌ها]، هیچکدام]] تمام [داده‌های توابع امنیتی هدف ارزیابی به جز داده‌های امنیتی رمزنگاری و زمان و تاریخی که به صورت مهر زمانی در حت-م.۱ استفاده می‌شود] به سرپرستان و موجودیت‌های IT مجاز (م‌د-م‌د.۱(۱))

۱۱. محدود کردن قابلیت تغییر دادن داده امنیتی رمزنگاری به سرپرست رمزنگاری (م‌د-م‌د.۱(۲))

۱۲. محدود کردن قابلیت تنظیم زمان و تاریخ استفاده شده به صورت مهرهای زمانی در حت-م.۱ به سرپرست‌های امنیتی یا موجودیت‌های IT مجاز.

۱۳. محدود کردن قابلیت پرس‌وجو، تغییر دادن، حذف کردن، ایجاد کردن، [انتخاب: [اختصاص: دیگر عملیات‌ها]، هیچکدام] قوانین مربوط به خط‌مشی جریان اطلاعات به سرپرست امنیتی (م‌د-م‌د.۱(۲))

۱۴. محدود کردن قابلیت تنظیم زمان و تاریخ استفاده شده به صورت مهرهای زمانی در حت-م.۱ به سرپرست‌های امنیتی یا موجودیت‌های IT مجاز (م‌د-م‌د.۱,۱(۳))

شماره الزام	نام خانواده	عنصر امنیتی

۱۵. محدود کردن قابلیت پرس و جو، تغییر دادن، حذف کردن، ایجاد کردن، [انتخاب:[اختصاص: دیگر عملیات‌ها]، هیچکدام] [قوانین مربوط به خط‌مشی جریان اطلاعات] به [سرپرست امنیتی] (م‌د-م‌د.۱,۱(۴))

۱۶. محدود کردن قابلیت لغو مشخصه‌های امنیتی مرتبط با [انتخاب: کاربران، موجودیت‌های فعال، موجودیت‌های غیر فعال، [اختصاص: دیگر منابع اضافی]] در داخل TSC به سرپرست‌های امنیتی

۱۷. محدود کردن مشخصات محدوده ظرفیت بر روی اتصالات لایه انتقال به سرپرست‌های امنیتی (م‌د-م‌د.۲(۱))

۱۸. محدود کردن مشخصات محدوده ظرفیت بر روی منابع اتصال‌گرای کنترل شده به سرپرست‌های امنیتی (م‌د-م‌د.۲(۲))

۱۹. محدود کردن مشخصات محدوده برای درصد ظرفیت ذخیره‌سازی برای رکوردهای ممیزی (م‌د-م‌د.۲(۳)) به سرپرست امنیتی

۲۰. محدود کردن قابلیت فعال کردن، غیرفعال کردن، تعیین و تغییر رفتار عملکرد اداره کردن شکست‌های احراز هویت(اش-ش‌ا.۲,۱.۱) تا تنظیم عدد صحیح مثبت و غیر صفر از تعداد تلاش‌های احراز هویت ناموفق مربوط به احراز هویت کاربر به سرپرست امنیتی

۲۱. [اختصاص: لیستی از عملکردهای مدیریتی امنیتی اضافی ارائه شده توسط محیط IT].

۶۵ **نام عنصر: محدودیت‌ها بر روی نقش‌های امنیتی ۲**

شماره مؤلفه: م‌د-ن‌م.۱,۲ (FMT_SMR.2.1)

شماره الزام	نام خانواده	عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید نقش‌های زیر را نگهداری نمایند:

- [نقش سرپرست امنیتی
- نقش سرپرست ممیزی
- نقش سرپرست رمزنگاری]

۶۶ **نام عنصر: محدودیت‌ها بر روی نقش‌های امنیتی ۲**

شماره مؤلفه: م‌د-ن‌م.۲,۲ (FMT_SMR.2.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به مرتبط کردن کاربران با نقش‌ها باشد.

۶۷ **نام عنصر: محدودیت‌ها بر روی نقش‌های امنیتی ۲**

شماره مؤلفه: م‌د-ن‌م.۳,۲ (FMT_SMR.2.3)

شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید این اطمینان را بدهد که شرایط [اختصاص: شرایط برای نقش‌های متفاوت] برآورده شده است.

نکته کاربردی:

سرپرستی هدف ارزیابی به قابلیت‌های مرتبط با نقش سرپرستی محدود می‌شود.

۷,۶ کلاس حفاظت از توابع امنیتی هدف ارزیابی

در ادامه المان‌های امنیتی مورد نیاز کلاس حفاظت از توابع امنیتی هدف ارزیابی ارائه شده است.

نام کلاس: حفاظت از توابع امنیتی هدف ارزیابی

شرح کلاس: این کلاس خانواده‌هایی از الزامات عملیاتی را در برمی‌گیرد که در ارتباط با صحت و مدیریت سازوکارهایی هستند که با توابع امنیتی هدف ارزیابی ترکیب می شوند و برای صحت و یکپارچگی داده توابع امنیتی هدف ارزیابی مورد استفاده قرار می‌گیرند. از بعضی جهات، خانواده‌های این کلاس ممکن است به نظر بیاید که تکرار عناصر کلاس محافظت از داده کاربری است، حتی ممکن است هر دوی این کلاس‌ها با سازوکار مشابهی پیاده‌سازی شده باشند. هرچند کلاس محافظت از داده کاربری بر روی محافظت از داده کاربری متمرکز شده است اما کلاس محافظت از توابع امنیتی هدف ارزیابی بر روی محافظت از داده‌های توابع امنیتی هدف ارزیابی متمرکز شده

است. در حقیقت، عناصر کلاس محافظت از توابع امنیتی هدف ارزیابی لازم است الزاماتی را ارائه نمایند که خط‌مشی‌های عملکرد امنیتی در هدف ارزیابی نتوانند مورد مداخله قرار بگیرند یا دور زده[1] شوند.

از دیدگاه این کلاس، باتوجه به توابع امنیتی هدف ارزیابی سه مؤلفه مهم وجود دارد:

- **پیاده‌سازی توابع امنیتی هدف ارزیابی،** که سازوکارهای اجرا کننده توابع امنیتی هدف ارزیابی را اجرا و پیاده‌سازی می‌کند.
- **داده توابع امنیتی هدف ارزیابی،** پایگاه داده‌های سرپرستی هستند که راهنمایی کننده اجرای عملکرد امنیتی می‌باشند.
- **موجودیت‌های خارجی** که توابع امنیتی هدف ارزیابی، ممکن است جهت اجرای الزامات عملکرد امنیتی با آن‌ها در تعامل باشند.

➢ خانواده شکست امن[2]

الزامات این خانواده اطمینان می‌دهد که هدف ارزیابی در هنگامی که مجموعه مشخصی از شکست‌ها در توابع امنیتی هدف ارزیابی روی می‌دهد، کارکرد امنیتی لازم اجرا می‌شود.

➢ خانواده دسترس‌پذیری داده ارسال شده توابع امنیتی هدف ارزیابی[3]

این خانواده قوانینی را تعریف می‌کند که از فقدان دسترسی داده، در هنگامی‌که بین توابع امنیتی هدف ارزیابی و دیگر محصولات IT منتقل می‌شود، جلوگیری کند. برای

1 Bypass

2 Fail secure(FPT_FLS)

3 Availability of exported TSF data(FPT_ITA)

مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[1]**

این خانواده تعریف کننده قوانینی برای محافظت از افشای غیرمجاز داده توابع امنیتی هدف ارزیابی در طول انتقال بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT می‌باشد. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[2]**

این خانواده تعریف کننده قوانینی برای حفاظت از تغییرات غیرمجاز داده‌های توابع امنیتی هدف ارزیابی است که بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شود. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی[3]**

این خانواده الزاماتی را ارائه می‌کند که از داده توابع امنیتی هدف ارزیابی در زمان انتقال بین بخش‌های مجزای توابع امنیتی هدف ارزیابی در سراسر کانال داخلی محافظت

1 Confidentiality of exported TSF data (FPT_ITC)

2 Integrity of exported TSF data (FPT_ITI)

3 Internal TOE TSF data transfer (FPT_ITT)

می‌کند.

➢ خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[1]

عناصر کلاس حفاظت فیزیکی توابع امنیتی هدف ارزیابی به محدود کردن دستیابی فیزیکی غیرمجاز به توابع امنیتی هدف ارزیابی، و هم‌چنین جلوگیری از/ مقاومت در برابر، تغییرات فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی اشاره دارند.

الزامات مطرح شده در عناصر این خانواده اطمینان می‌دهند که از توابع امنیتی هدف ارزیابی در برابر مداخله فیزیکی و تداخلات محافظت می‌شود. ارضاء شدن این عناصر منجر به بسته‌بندی و استفاده توابع امنیتی هدف ارزیابی به صورتی می‌شود که مداخلات فیزیکی قابل تشخیص باشند یا مجبور به مقاومت در برابر تداخلات فیزیکی شوند. بدون این عناصر، عملکرد حفاظت از توابع امنیتی هدف ارزیابی اثرشان را در محیط‌هایی که از آسیب فیزیکی نمی‌توانند جلوگیری نمایند، از دست می‌دهند بنابراین این خانواده چنین الزاماتی را ارائه نموده است که چطور توابع امنیتی هدف ارزیابی باید به تلاش‌هایی که در ارتباط با تداخل فیزیکی صورت می‌گیرد، واکنش نشان دهند.

➢ خانواده بازیابی مطمئن[2]

الزامات این خانواده اطمینان می‌دهند که توابع امنیتی هدف ارزیابی می‌توانند تشخیص دهند که هدف ارزیابی بعد از قطع عملیات، بدون به خطر افتادن حفاظت می‌تواند راه‌اندازی و بازیابی شود. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی، تعیین کننده حفاظت از وضعیت‌های بعدی می‌باشد.

➢ خانواده تشخیص مجدد[1]

---

1 TSF physical protection (FPT_PHP)

2 Trusted recovery (FPT_RCV)

این خانواده تکرار شدن انواع مختلف موجودیت‌ها (به طور مثال، پیغام‌ها، درخواست‌های سرویس، پاسخ‌های سرویس) و صحت اقدامات بعدی را تشخیص می‌دهد. با توجه به این الزام در مواردی که تکرار تشخیص داده شوند، ممکن است از این امر جلوگیری به عمل آید.

- **خانواده پروتکل هم‌زمانی حالت[۲]**

هدف‌های ارزیابی که توزیع شده‌اند ممکن است نسبت به هدف ارزیابی واحد، به واسطه اختلاف پتانسیل در حالت بین بخش‌های مختلف هدف ارزیابی و تاخیر در ارتباطات دارای پیچیدگی بیشتر باشد. در اغلب موارد هم‌زمانی حالت‌ها بین عملکردهای توزیع یافته مستلزم یک پروتکل تبادلی است و به سادگی صورت نمی‌گیرد.

در حالتی که به محیط توزیعی این پروتکل‌ها اعتمادی نباشد، به پروتکل هم‌زمانی پیچیده‌تری نیاز است.

پروتکل هم‌زمانی حالت، الزاماتی را برای عملکردهای بحرانی خاص مربوط به تابع امنیتی هدف ارزیابی ایجاد می‌کند تا از این پروتکل امن استفاده نمایند. پروتکل هم‌زمانی اطمینان می‌دهد که دو بخش توزیعی هدف ارزیابی (به طور مثال، میزبان‌ها) حالت‌هایشان را بعد از اقدامات مرتبط امنیتی هم‌زمان می‌نمایند.

- **خانواده مهرهای زمانی[۳]**

این خانواده، الزاماتی را برای یک مهر زمانی معتبر در داخل هدف ارزیابی، نشان می‌دهد.

- **خانواده هم‌خوانی داده‌های بین توابع امنیتی هدف ارزیابی[۴]**

---

1 Replay detection (FPT_RPL)

2 State synchrony protocol (FPT_SSP)

3 Time stamps (FPT_STM)

4 Inter-TSF TSF data consistency

در یک محیط توزیعی، هدف ارزیابی ممکن است به تبادل داده توابع امنیتی هدف ارزیابی (صفات خط مشی عملکرد امنیتی که به داده اختصاص یافته، اطلاعات ممیزی، اطلاعات شناسایی) با دیگر محصولات امن IT نیاز داشته باشد. این خانواده الزاماتی را برای به اشتراک گذاری و تفسیر سازگار صفات و مجوزها، بین توابع امنیتی هدف ارزیابی مربوط به هدف ارزیابی و یک محصول امن IT متفاوت تعریف می‌کند.

- **خانواده آزمون موجودیت‌های خارجی[1]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف می‌کند تا آزمون‌هایی را بر روی یک یا بیش از یک موجودیت خارجی انجام دهند. عناصر مطرح شده در این خانواده برای اعمال به کاربران انسانی در نظر گرفته نشده‌اند.

موجودیت‌های خارجی، ممکن است شامل برنامه‌هایی باشند که بر روی هدف ارزیابی اجرا می‌شوند، سخت‌افزار و نرم‌افزاری که تحت هدف ارزیابی اجرا می‌شود(پلتفرم‌ها، سیستم‌عامل و ...) یا برنامه‌ها و باکس‌های متصل شده به هدف ارزیابی (سیستم‌های تشخیص نفوذ، دیوارهای آتش، سرورهای ورود، سرورهای زمانی و غیره) باشد.

- **خانواده هم‌خوانی تکرار داده‌ها در توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی[2]**

الزامات این خانواده از آن جهت لازم و ضروری می‌باشد، تا از هم‌خوانی داده توابع امنیتی هدف ارزیابی زمانی‌که در داخل هدف ارزیابی تکرار می‌شود، اطمینان حاصل کند. منظور از هم‌خوانی داده‌ها، یکسان بودن داده‌ها در محل‌ها و توابع مختلف است. داده توابع امنیتی هدف ارزیابی زمانی ناهم‌خوان می‌شود که کانال داخلی بین بخش‌های

1 Testing of external entities(FPT_TEE)

2 Internal TOE TSF data replication consistency(FPT_TRC)

مختلف هدف ارزیابی نامعتبر شود. اگر اجزای هدف ارزیابی از نظر داخلی تشکیل یک شبکه دهند، در صورت غیر فعال شدن ارتباطات شبکه‌ای، عدم هم‌خوانی بین داده-های تابع امنیتی می‌تواند رخ دهد.

➢ خانواده خودآزمایی توابع امنیتی هدف ارزیابی[1]

این خانواده الزاماتی را برای خودآزمایی توابع امنیتی هدف ارزیابی با توجه به عملکرد صحیح مورد انتظار تعریف می‌کند. اجبار هدف ارزیابی به انجام آزمون بر روی بخش-های حساس و مهم هدف ارزیابی با استفاده از نمونه عملیات‌های ریاضی مثالی از این الزام می باشد. این‌گونه آزمون‌ها می‌تواند در هنگام راه اندازی، به طور متناوب بنا به درخواست کاربر مجاز، یا در زمانی‌که شرایط خاصی ایجاد شود، انجام گیرد. عملی که باید به عنوان نتیجه خودآزمایی توسط هدف ارزیابی انجام شود در دیگر خانواده‌ها تعریف می‌شود.

الزامات این خانواده هم‌چنین برای تشخیص عدم صحت داده توابع امنیتی هدف ارزیابی یا خود توابع امنیتی هدف ارزیابی (کد اجرایی یا مؤلفه‌های سخت‌افزاری توابع امنیتی هدف ارزیابی) توسط خرابی‌های مختلفی که لزوماً عملکرد هدف ارزیابی (که توسط دیگر خانواده‌ها اداره شده‌اند) را متوقف نمی‌کنند، مورد نیاز است.

چنین خرابی‌هایی می‌تواند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط در طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهد یا به دلیل تغییر مخرب توابع امنیتی هدف ارزیابی بر اثر حفاظت منطقی و/یا فیزیکی ناکافی صورت گیرد.

1 TSF self test(FPT_TST)

شماره	نام خانواده	عنصر امنیتی
الزام		
۶۸	نقض امنیت (FPT_FLS)	**نام عنصر: شکست با حفظ کردن حالت امن ۱** **شماره مؤلفه: ح‌ت-ن‌ا.۱,۱(FPT_FLS.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید زمانی‌که انواع شکست‌های زیر رخ می‌دهد، در یک وضعیت امن حفظ شود.
۶۹	در دسترس بودن داده-های ارسال شده توابع امنیتی هدف ارزیابی (FPT_ITA)	**نام عنصر: در دسترس بودن بین توابع امنیتی هدف ارزیابی توسط معیارهای مشخص ۱** **شماره مؤلفه: ح‌ت-دد.۱,۱(FPT_ITA.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از در دسترس بودن [اختصاص: لیستی از انواع داده‌های توابع امنیتی هدف ارزیابی] که برای دیگر محصولات معتبرِ IT به صورت راه دور ارسال می نمایند، بر اساس [اختصاص: معیارهای مشخص در جهت اطمینان از ارائه دسترسی]، تحت شرایط[اختصاص: شرایطی که تضمین‌کننده دسترسی داده‌ها می‌باشد] اطمینان حاصل کنند. **نکته کاربردی:** مسیریاب باید نسبت به پیروی کردن مشخصات برای پروتکل‌های مسیریابی مختلف که برای ارسال مجدد و دسترس پذیری داده‌های

شماره الزام	نام خانواده	عنصر امنیتی
		مسیریابی به مسیریاب‌های همتا استفاده می‌شود، اطمینان یابد.
۷۰	محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی (FPT_ITC)	**نام عنصر: محرمانگی داده‌های ارسال شده بین توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: ح‌ت-م‌د.۱،۱(FPT_ITC.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از کلیه داده‌های انتقال یافته از خود به دیگر محصولات معتبرِ IT راه دور، در مقابل آشکارسازی و افشای غیرمجاز، در طول فرآیند انتقال، محافظت کند. **نکته کاربردی:** این الزام از مسیریابی و مسیریابی مربوط به بروزرسانی‌های بین دو مسیریاب محافظت می‌کند. یک مثال استفاده از پروتکل اینترنت نسخه ۶ (IPv6) و پروتکل اینترنت امنیتی (IPSEC) می‌باشد، به گونه‌ای که یک مسیریاب می‌تواند جدول مسیریابی ارتباطات و احرازهویت با مسیریاب همتا را رمزنگاری کند. این روشی است که از محرمانگی منابع شبکه محافظت می‌کند.
۷۱	یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی	**نام عنصر: تشخیص تغییرات بین توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: ح‌ت-ی‌د.۱،۱ (FPT_ITI.1.1)**

شماره	نام خانواده	عنصر امنیتی
	الزام (FPT_ITI)	شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید بر اساس [اختصاص: معیار تغییر تعریف‌شده]، در هنگام نقل و انتقال داده‌ها بین خود و محصولات معتبر IT راه دور، قادر به شناسایی تغییرات در تمام داده‌ها باشند.

۷۲ **نام عنصر: تشخیص تغییرات بین توابع امنیتی هدف ارزیابی ۱**

شماره مؤلفه: ح‌ت-ی‌د.۲,۱ (FPT_ITI.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید توانایی بررسی یکپارچگی تمام داده‌های توابع امنیتی هدف ارزیابی که در حال انتقال بین توابع خود و محصولات معتبر IT راه دور، می‌باشند را فراهم نموده و در صورت تشخیص تغییرات، [اختصاص: اقدامات مشخصی] را انجام دهند.

نکته کاربردی:

این الزام از مسیریابی و مسیریابی مربوط به بروزرسانی‌های بین دو مسیریاب محافظت می‌کند. یک مثال استفاده از پروتکل اینترنت نسخه ۶ (IPv6) و پروتکل اینترنت امنیتی (IPSEC) می‌باشد، به گونه‌ای که یک مسیریاب می‌تواند ارتباطات همتا را به وسیله رمزنگاری جدول مسیریابی ارتباطات و احرازهویت با مسیریاب همتا ، محافظت و آشکارسازی کند.

شماره	نام خانواده	عنصر امنیتی
الزام		
۷۳	اسنفاده از پروتکل استاندارد(توسعه یافته) **(FPT_PRO_(EXT))** ۰)	**نام عنصر: استفاده از پروتکل استاندارد(ت‌س) ۱** **شماره مؤلفه:** ح‌ت-اب-(ت‌س).**۱,۱ (FPT_PRO_(EXT).1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از سازوکارهای پروتکل استاندارد در داخل پروتکل‌های استاندارد استفاده کند. [انتخاب: [اختصاص: • BGP • لیستی از پروتکل‌های استاندارد]].
۷۴	محافظت از داده توابع امنیتی هدف ارزیابی(توسعه یافته) **(FPT_SKP_EXT)**	**نام عنصر: محافظت از داده‌های توابع امنیتی هدف ارزیابی (کلیدهای متقارن) ۱** **شماره مؤلفه: ح‌ت-مح-(ت‌س).۱,۱(FPT_SKP_EXT)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از خوانده شدن تمام کلیدهای از پیش به اشتراک گذارده شده، کلیدهای متقارن و کلیدهای خصوصی جلوگیری کند. **نکته کاربردی:**

شماره	نام خانواده	عنصر امنیتی
	الزام	منظور این الزام آن است که یک سرپرست قادر به خواندن یا مشاهده کلیدهای شناسایی شده از طریق واسطهای «معمول» نمی‌باشد. درحالی‌که قابل درک است که سرپرست می‌تواند برای مشاهده این کلیدها، مستقیماً حافظه را بخواند. از این‌رو سرپرست به عنوان یک عامل امن در نظر گرفته می‌شود و فرض می‌شود که تلاشی در این مورد نمی‌کند.
۷۵	حفاظت از کلمه‌های عبور سرپرست **(FPT_APW_EXT)**	**نام عنصر: حفاظت از کلمه‌های عبور سرپرست ۱** **شماره مؤلفه: ح‌ت-م‌پ-(ت‌س).۱,۱ (FPT_APW_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید کلمه‌های عبور را به صورت متن آشکار ذخیره نکند.
۷۶		**نام عنصر: حفاظت از کلمه‌های عبور سرپرست ۱** **شماره مؤلفه: ح‌ت-م‌پ-(ت‌س).۲,۱ (FPT_APW_EXT.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از خواندن کلمه‌های عبور به صورت متن آشکار جلوگیری کند. **نکته کاربردی:**

شماره نام خانواده

الزام

عنصر امنیتی

منظور این الزام آن است که داده‌های مربوط برای احراز هویت به صورت متن آشکار ذخیره نشوند و هیچ کاربر و سرپرستی قادر به خواندن کلمه عبور به صورت متن آشکار از طریق واسط‌های معمول نمی‌باشد. سرپرست اصلی هدف ارزیابی قطعا می‌تواند کلمه عبور را مستقیماً از حافظه بازیابی کند، اما از آنجا که مورد اعتماد است این کار را انجام نمی‌دهد. در این نسخه از پروفایل حفاظتی الزامی بر روی روش مورد استفاده جهت ذخیره کلمه عبور به صورت غیر متنی وجود ندارد، اما مرجع روش‌های رمزنگاری در الزام «رز-ع ر» پیشنهاد داده می‌شوند.

۷۷ بازیابی مطمئن **(FPT_RCV)**

نام عنصر: بازیابی خودکار ۲

شماره مؤلفه: ح‌ت-ب‌م.۱,۲(FPT_RCV.2.1)

شرح مؤلفه:

زمانی‌که بازیابی خودکار از [اختصاص: لیستی از شکست‌ها/سرویس‌های منقطع] امکان‌پذیر نمی‌باشد، توابع امنیتی هدف ارزیابی باید وارد یک حالت نگهداری[1] شود که بتواند به یک حالت امن فراهم شده برشود.

۷۸ **نام عنصر: بازیابی خودکار ۲**

1 Maintenance mode

شماره	نام خانواده	عنصر امنیتی
	الزام	
		شماره مؤلفه: ح‌ت-ب‌م.۲,۲(FPT_RCV.2.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید این اطمینان را بدهند که برای [اختصاص: لیستی از شکست‌ها/سرویس‌های منقطع]، هدف ارزیابی را با استفاده از رویه‌های خودکار به یک حالت امن برمی‌گردانند.
۷۹	شناسایی مجدد (FPT_RPL)	**نام عنصر: آشکارسازی مجدد ۱**
		شماره مؤلفه: ح‌ت-ش‌م.۱,۱(FPT_RPL.1.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید تکرار شدن موجودیت‌های زیر را آشکارسازی کنند: [داده توابع امنیتی هدف ارزیابی و ویژگی‌های امنیتی]
۸۰		**نام عنصر: آشکارسازی مجدد ۱**
		شماره مؤلفه: ح‌ت-ش‌م.۲,۱(FPT_RPL.1.2)
		شرح مؤلفه:

شماره	نام خانواده	عنصر امنیتی
	الزام	توابع امنیتی هدف ارزیابی، باید در زمان آشکارسازی مجدد اقدامات زیر را انجام دهند: [• رد کردن داده‌ها؛ • ممیزی رویداد؛ • [انتخاب: [اختصاص: لیستی از اقدامات خاص،] هیچکدام]]. **نکته کاربردی:** دریافت بسته‌های شبکه متعدد با توجه به تراکم شبکه یا تصدیق‌های بسته از دست داده شده ، به عنوان یک حمله مجدد در نظر گرفته نمی‌شود. هدف از این الزام آن است تا اطمینان حاصل شود که نشست اداری(در بخش، در تمامیت آن، توسط یک مدیر از راه دور یا یک نهاد IT مجاز) یا دنباله احراز هویت کاربر نمی‌تواند تکرار شود.
۸۱	مهرهای زمانی قابل اطمینان **(FPT_STM.)**	**نام عنصر: مهرهای زمانی قابل اطمینان ۱** **شماره مؤلفه: ح‌ت-م‌ز.۱،۱(FPT_STM.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید قادر به ایجاد مهرهای زمانی قابل اطمینان برای استفاده **هدف ارزیابی** باشند.
۸۲	سازگاری داده‌های توابع امنیتی هدف ارزیابی بین توابع	**نام عنصر:** سازگاری داده‌های توابع امنیتی هدف ارزیابی بین توابع امنیتی هدف ارزیابی **۱** **شماره مؤلفه: ح‌ت-س‌د.۱،۱(FPT_TDC.1.1)**

شماره	نام خانواده	عنصر امنیتی
الزام		
	امنیتی هدف ارزیابی (FPT_TDC)	**شرح مؤلفه:**
		توابع امنیتی هدف ارزیابی باید قادر باشند [اختصاص: لیستی از انواع داده‌های توابع امنیتی هدف ارزیابی] را زمانی‌که بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT به اشتراک گذاشته می‌شود، به طور مداوم تفسیر نمایند.
۸۳		**نام عنصر:** سازگاری داده‌های توابع امنیتی هدف ارزیابی بین توابع امنیتی هدف ارزیابی **۱**
		شماره مؤلفه: ح‌ت-س‌د.۲,۱.(FPT_TDC.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید [اختصاص: لیستی از قوانین تفسیر اعمال شده توسط توابع امنیتی هدف ارزیابی] استفاده نمایند، زمانی‌که داده توابع امنیتی هدف ارزیابی از دیگر محصولات امن IT تفسیر می‌شود.
۸۴	به روز رسانی امن (FPT_TUD_EXT)	**نام عنصر : به روز رسانی امن ۱**
		شماره مؤلفه: ح‌ت-رم-(ت‌س).۱,۱.(FPT_TUD_EXT.1.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید به سرپرستان امنیتی این قابلیت را بدهند تا بتوانند نسخه فعلی نرم افزار/میان افزار هدف ارزیابی را پرس

شماره	نام خانواده الزام	عنصر امنیتی
		و جو و مشاهده نمایند.
۸۵		**نام عنصر : به روز رسانی امن ۱**
		شماره مؤلفه: ح‌ت-رم-(ت‌س).۲,۱(FPT_TUD_EXT.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید به سرپرستان امنیتی این قابلیت را بدهند تا بتوانند فرایند به روز رسانی نرم افزار/میان افزار هدف ارزیابی را انجام دهند.
۸۶		**نام عنصر : به روز رسانی امن ۱**
		شماره مؤلفه: ح‌ت-رم-(ت‌س).۳,۱(FPT_TUD_EXT.1.3)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید به وسیله روشی قبل از به روز رسانی هدف ارزیابی، با استفاده از [انتخاب: سازوکارهای امضای دیجیتال، مقادیر درهم‌سازی منتشر شده] از صحت به روز رسانی نرم افزاری/میان افزاری اطمینان حاصل نمایند.
		نکته کاربردی:

شماره	نام خانواده الزام	عنصر امنیتی
		سازوکار امضای دیجیتال اشاره به سومین عنصر مشخص شده در مؤلفه رز-ع ر.۱(۲) دارد.
		مقادیر درهم‌سازی منتشرشده توسط یکی از توابع مشخص شده در رز-ع ر.۱(۳) تولید می‌شود.
		نویسنده هدف امنیتی باید سازوکارهای پیاده‌سازی شده توسط هدف ارزیابی را انتخاب کند.
۸۷	خودآزمایی توابع امنیتی هدف ارزیابی (FPT_TST_EXP)	**نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: حت-خا-(ت‌س).۱٫۱(FPT_TST_EXP.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید مجموعه‌ای از خودآزمایی‌ها را در حین راه‌اندازی اولیه و هم‌چنین به صورت دوره‌ای در حین عملیات عادی سیستم، یا در زمان درخواست از کاربر مجاز اجرا نمایند، تا نشان‌دهنده عملکرد صحیح توابع امنیتی هدف ارزیابی باشد.
۸۸		**نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: حت-خا-(ت‌س).۱٫۲(FPT_TST_EXP.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت تائید یکپارچگی و صحت کد اجرایی ذخیره‌شده توابع امنیتی هدف ارزیابی را از طریق استفاده از

شماره نام خانواده

عنصر امنیتی

الزام

سرویس‌های رمزنگاری ارائه شده برای سرپرستان مجاز فراهم کند.

نکته کاربردی:

برای سرویس‌های رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی اشاره به رز-ع‌ر.۱,۱.(۲) و رز-ع‌ر.۱,۱.(۳) دارد.

۸۹ **نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی**(برای رمزنگاری) **۱ (۱)**

شماره مؤلفه: ح‌ت-خ‌ا.۱,۱.(۱) ((FPT_TST.1.1 (1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مجموعه‌ای از خودآزمایی‌ها را مطابق با FIPS PUB 140-2 و پیوست این پروفایل در حین راه‌اندازی اولیه(یا روشن شدن)، یا در زمان درخواست از کاربر مجاز، تحت شرایط مختلفی که در بخش ۴,۹,۱ از FIPS 140-2 تعریف شده است، به طور متناوب (حداقل یکبار در روز) اجرا کند، تا نشان‌دهنده عملکرد صحیح توابع رمزنگاری زیر باشد:

- تشخیص خطای کلید
- الگوریتم‌های رمزنگاری
- PNG/PRNG

شماره نام خانواده

الزام

عنصر امنیتی

نکته کاربردی:

این آزمون بدون در نظر گرفتن آنکه عملکرد رمزنگاری در سخت‌افزار، نرم‌افزار یا میان افزار پیاده‌سازی شده است، صورت می‌گیرد.

۹۰ **نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی**(برای رمزنگاری) **۱ (۱)**

شماره مؤلفه: ح‌ت-خ‌ا.۲,۱.۱(۱) ((FPT_TST.1.2 (1))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت تائید یکپارچگی داده‌های توابع امنیتی هدف ارزیابی مربوط به رمزنگاری را با استفاده از عملکرد رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی برای سرپرستان رمزنگاری مجاز ارائه کند.

نکته کاربردی:

برای سرویس‌های رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی اشاره به رز-ع‌ر.۱,۱.۱(۲) و رز-ع‌ر.۱,۱.۱(۳) دارد.

۹۱ **نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی**(برای رمزنگاری) **۱ (۱)**

شماره مؤلفه: ح‌ت-خ‌ا.۳,۱.۱(۱) ((FPT_TST.1.3 (1))

شرح مؤلفه:

شماره نام خانواده

الزام

عنصر امنیتی

توابع امنیتی هدف ارزیابی باید تائید یکپارچگی کد اجرایی ذخیره‌شده توابع امنیتی هدف ارزیابی مربوط به رمزنگاری را با استفاده از عملکردهای رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی برای سرپرستان رمزنگاری مجاز فراهم کند.

۹۲ **نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی**(برای عناصر تولید کلید) **۱ (۲)**

شماره مؤلفه: ح‌ت-خ‌ا.۱,۱(۲) ((FPT_TST.1.1 (2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید آزمون‌های خودآزمایی را باید بلافاصله پس از تولید کلید اجرا کند تا عملکرد صحیح هریک از مؤلفه‌های تولید کلید را نشان دهد. اگر هر کدام از این آزمون‌ها با شکست مواجه شود، کلید تولید شده نباید مورد استفاده قرار بگیرد، ماژول رمزنگاری باید در صورت نیاز توسط FIPS PUB 140-2 به خودآزمایی‌های منجر به شکست، عکس العمل نشان دهد و این رویداد ممیزی شود.

نکته کاربردی:

مؤلفه‌های تولید کلید عناصر حیاتی هستند که تشکیل دهنده تمام رویه تولید کلید می‌باشند(به طور مثال، هر الگوریتم، PNG/PRNG، هر کلید تولید شده.).

شماره نام خانواده

الزام

عنصر امنیتی

این آزمون‌های خودآزمایی بر روی مؤلفه‌های تولید کلید، می‌تواند در اینجا به صورت یک زیرمجموعه از مجموعه کامل آزمون‌های خودآزمایی اجراشده بر روی رمزنگاری در حت-خا، تا زمانی‌که تمام عناصر رویه تولید کلید مورد آزمون قرار گیرند؛ اجرا شود.

۹۳ **نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی**(برای عناصر تولید کلید) **۱ (۲)**

شماره مؤلفه: حت-خا.۲,۱.۱(۲) ((FPT_TST.1.2 (2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت تائید یکپارچگی داده‌های توابع امنیتی هدف ارزیابی مربوط به تولید کلید را با استفاده از عملکرد رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی به سرپرستان رمزنگاری مجاز ارائه کند.

نکته کاربردی:

برای سرویس‌های رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی اشاره به رز-ع‌ر.۱,۱(۲) و رز-ع‌ر.۱,۱(۳) دارد.

۹۴ **نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی**(برای عناصر تولید کلید) **۱ (۲)**

شماره مؤلفه: حت-خا.۳,۱.۱(۲) ((FPT_TST.1.3 (2))

شرح مؤلفه:

شماره نام خانواده	عنصر امنیتی
الزام	توابع امنیتی هدف ارزیابی باید قابلیت تائید یکپارچگی کد اجرایی ذخیره‌شده توابع امنیتی هدف ارزیابی مربوط به تولید کلید را با استفاده از عملکردهای رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی برای سرپرستان رمزنگاری مجاز فراهم کند.
	نکته کاربردی:
	برای سرویس‌های رمزنگاری ارائه شده توسط توابع امنیتی هدف ارزیابی اشاره به رز-ع‌ر.۱،۱.(۲) و رز-ع‌ر.۱،۱.(۳) دارد.

۷،۷ کلاس استفاده از منابع

در ادامه المان‌های امنیتی مورد نیاز کلاس منابع مورد استفاده ارائه شده است.

نام کلاس: تخصیص منابع

شرح کلاس: این کلاس ارائه کننده سه خانواده است که از دسترس‌پذیری منابع لازم هم‌چون قابلیت پردازش و/یا ظرفیت ذخیره‌سازی پشتیبانی می‌کند. خانواده‌ی تحمل خرابی، ارائه کننده حفاظت درقبال غیرقابل دسترس بودن قابلیت‌های ناشی از شکست هدف ارزیابی است. خانواده‌ی اولویت سرویس اطمینان خواهد داد که منابع به فعالیت‌های خیلی مهم یا زمان بحرانی تخصیص داده می‌شود و فعالیت‌های با اولویت پائین‌تر نمی‌توانند این سرویس‌ها را به انحصار خود درآورند. خانواده‌ی تخصیص منابع، محدودیت‌هایی را بر روی استفاده از منابع در دسترس اعمال می‌کند بنابراین از انحصار منابع توسط کاربران جلوگیری می‌کند.

- **خانواده تحمل خرابی**

الزامات این خانواده اطمینان می‌دهد که هدف ارزیابی حتی در زمان روی‌دادن یک رخداد شکست، از عملکرد صحیح‌اش نگهداری خواهد کرد.

- **خانواده اولویت سرویس**

الزامات این خانواده به توابع امنیتی هدف ارزیابی اجازه می‌دهد تا استفاده از منابع تحت کنترل توابع امنیتی هدف ارزیابی را توسط کاربران و موجودیت‌های فعالی کنترل کند به گونه‌ای که فعالیت‌های با اولویت بالا تحت کنترل توابع امنیتی هدف ارزیابی همواره بدون مداخله‌های غیرضروری یا تأخیر ناشی از فعالیت‌های با اولویت پایین انجام می‌شوند.

- **خانواده تخصیص منابع**

الزامات این خانواده به توابع امنیتی هدف ارزیابی اجازه می‌دهد تا استفاده از منابع را توسط کاربران و موجودیت‌های فعال کنترل کند به طوری‌که انکار سرویس به دلیل انحصارگرایی غیرمجاز منابع رخ نخواهد داد.

شماره الزام	نام خانواده	عنصر امنیتی
۹۵	تخصیص منابع (FRU_RSA)	**نام عنصر: حداکثر ظرفیت (ظرفیت لایه انتقال)** **شماره مؤلفه: من-ت‌م.۱،۱(۱) ((FRU_RSA.1.1(1))** **شرح مؤلفه:**

شماره	نام خانواده	عنصر امنیتی
	الزام	

توابع امنیتی هدف ارزیابی باید حداکثر ظرفیت منابع زیر را اجرا کند:

[نمایش لایه انتقال] که یک شناسه موجودیت فعال مبدأ می‌تواند بیش از بازه زمانی مشخص شده استفاده شود.

نکته کاربردی:

"نمایش لایه انتقال" به طور خاص به حملات TCP SYN اشاره دارد، در جایی که اتصالات نیمه باز برقرار شده است، بنابراین جدول اتصالات منابع را تهی می‌کند. انتخابات برای این الزام پالایش می‌شود تا شناسه موجودیت فعال منبع را مشخص کند که خیلی دقیق‌تر از کاربر یا موجودیت فعال در زمینه مسیریاب است. چنان‌چه هدف ارزیابی، پروتکل TCP/IP را پیاده‌سازی نکند، این الزام نوع مشابهی از موجودیت لایه انتقال برای پشته پروتکل هدف ارزیابی اعمال می‌کند.

۹۶ **نام عنصر: حداکثر ظرفیت (ظرفیت اتصال گرای کنترل شده)**

شماره مؤلفه: مn-ت‌م.۱,۱(۲) ((FRU_RSA.1.1(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید حداکثر ظرفیت منابع [منابع اتصال‌گرای کنترل شده] را که توسط سرپرست مشخص شده است اجرا کند که کاربران مرتبط با [شناسه شبکه مشخص شده توسط سرپرست و مجموعه‌ای از شناسه‌های شبکه مشخص شده توسط

شماره نام خانواده

عنصر امنیتی

الزام

سرپرست] بتوانند بیش از دوره زمانی مشخص شده توسط سرپرست استفاده کنند.

نکته کاربردی:

****

۷,۸ کلاس دسترسی به هدف ارزیابی

در ادامه المان‌های امنیتی مورد نیاز کلاس دسترسی به هدف ارزیابی ارائه شده است.

نام کلاس: دسترسی به هدف ارزیابی

شرح کلاس: این خانواده الزامات عملیاتی را برای کنترل نشست‌های کاربری برقرار شده مشخص می‌کند.

- **خانواده محدودیت دامنه‌ی ویژگی‌های قابل انتخاب**[1]

این خانواده الزاماتی را تعریف می‌کند تا دامنه‌ی صفات و ویژگی‌های امنیتی نشست را که یک کاربر ممکن است برای یک نشست انتخاب کند محدود کند.

- **خانواده محدودیت برای نشست‌های هم‌زمان چندگانه**[1]

1 Limitation on scope of selectable attributes(FTA_LSA)

این خانواده الزاماتی را تعریف می‌کند که تعداد نشست‌های هم‌زمان را که متعلق به یک کاربر است محدود کند.

- **قفل کردن و خاتمه دادن نشست[۲]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف کرده است تا قابلیتی را برای قفل کردن، باز کردن و خاتمه نشست‌های تعاملی که توسط توابع امنیتی هدف ارزیابی و کاربر آغاز شده است تعریف کند.

- **علائم دسترسی هدف ارزیابی[۳]**

این خانواده تعریف کننده الزاماتی است تا یک پیغام هشدار مشورتی قابل تنظیم را به کاربران با توجه به استفاده مناسب از هدف ارزیابی نمایش دهد.

- **سوابق دسترسی به هدف ارزیابی[۴]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف کرده است تا برای نشست‌هایی که موفقیت آمیز برقرار شده است، تاریخچه تلاش‌های موفق و ناموفق دستیابی به حساب کاربری را به کاربر نمایش دهد.

- **برقراری نشست هدف ارزیابی[۵]**

---

1 Limitation on multiple concurrent sessions(FTA_MCS)

2 Session locking and termination(FTA_SSL)

3 TOE access banners(FTA_TAB)

4 TOE access history(FTA_TAH)

5 TOE session establishment(FTA_TSE)

این خانواده الزاماتی را تعریف می‌کند تا مجوز کاربری را جهت برقراری یک نشست با هدف ارزیابی انکار کند.

شماره الزام	نام خانواده	عنصر امنیتی
۹۷	قفل کردن نشست-های شروع شده توسط توابع امنیتی هدف ارزیابی (FTA_SSL)	**نام عنصر: قفل کردن نشست های شروع شده توسط توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه:دس-ق‌ن.(ت‌س).۱,۱(FTA_SSL_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید برای نشست‌های تعاملی محلی پس از یک دوره زمانی غیرفعال مشخص تعریف شده توسط سرپرست امنیت [انتخاب: ۱. قفل کردن نشست - غیرفعال‌سازی کلیه فعالیت‌های مربوط به دسترسی داده‌های کاربر/دستگاه‌های نمایش به غیر از اینکه نیاز است قبل از باز کردن نشست، توابع امنیتی هدف ارزیابی، سرپرست را دوباره احرازهویت کند. ۲. خاتمه دادن نشست] .
۹۸		**نام عنصر: قفل کردن نشست‌های شروع شده توسط توابع امنیتی هدف ارزیابی ۳** **شماره مؤلفه:دس-ق‌ن.۱,۳ (FTA_SSL.3.1)** **شرح مؤلفه:**

شماره	نام خانواده الزام	عنصر امنیتی
		توابع امنیتی هدف ارزیابی باید نشست تعاملی راه دور [1]را پس از [بازه زمانی نشست غیرفعال قابل پیکربندی توسط سرپرست امنیت] خاتمه دهد.
۹۹		**نام عنصر: قفل کردن نشست‌های شروع شده توسط توابع امنیتی هدف ارزیابی ۴** **شماره مؤلفه:دس-ق‌ن. ۱,۴(FTA_SSL.4.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به شروع کننده نشست اجازه اتمام نشست تعاملی خودش را بدهد.
۱۰۰	علائم دسترسی هدف ارزیابی **(FTA_TAB)**	**نام عنصر: علایم دسترسی هدف ارزیابی پیش‌فرض ۱** **شماره مؤلفه: دس-ع‌د.۱,۱(FTA_TAB.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پیش از آغاز نشست کاربری سرپرستی، یک پیام هشدار مشخص شده توسط سرپرست امنیت را که بیانگر استفاده از هدف ارزیابی است نمایش دهد.

1 Remote

شماره	نام خانواده الزام	عنصر امنیتی

نکته کاربردی:

این الزام برای اعمال به نشست‌های تعاملی بین کاربر انسانی و هدف ارزیابی درنظر گرفته شده است. نیازی نیست موجودیت‌های فناوری اطلاعاتی که اتصالات معمولی یا اتصالات برنامه‌ریزی شده (مثل فراخوانی‌های رویه راه دور[1] بر روی شبکه) برقرار می‌کنند توسط این الزام پوشش داده شوند.

علامت دسترسی زمانی‌که هدف ارزیابی اعلانی مبنی بر شناسایی و احراز هویت ارائه دهد، به کار می‌رود. هدف از این الزام آگاهی دادن به کاربران در خصوص هشدارهای مربوط به استفاده غیر مجاز از هدف ارزیابی و فراهم آوردن امنیت سرپرستی با کنترل آن‌چه که نمایش داده می‌شود، خواهد بود(به طور مثال اگر سرپرست امنیت انتخاب کند، می‌توانند اطلاعات علائم را که کاربر محصول و شماره نسخه را اطلاع می‌دهد، حذف کنند).

۱۰۱	ایجاد نشست هدف ارزیابی **(FTA_TSE)**	**نام عنصر: ایجاد نشست هدف ارزیابی ۱** شماره مؤلفه: **دس-ان.۱,۱(FTA_TSE.1.1)** شرح مؤلفه:

1 Remote procedure calls

شماره	نام خانواده	عنصر امنیتی
الزام		

توابع امنیتی هدف ارزیابی، باید قادر به انکار نشست‌های ایجاد شده براساس [اختصاص: ویژگی‌ها] باشد.

۷,۹ کلاس کانال‌ها و مسیرهای مورد اعتماد

در ادامه المان‌های امنیتی مورد نیاز کلاس کانال‌ها و مسیرهای مورد اعتماد ارائه شده است.

نام کلاس: کانال‌ها و مسیرهای مورد اعتماد

شرح کلاس: خانواده‌های این کلاس الزاماتی را برای یک مسیر ارتباطی امن بین کاربران و توابع امنیتی هدف ارزیابی تعریف کرده‌اند هم‌چنین الزاماتی را برای یک کانال ارتباطی امن بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT ارائه کرده‌اند. مسیر و کانال امن دارای شاخصه‌های اصلی زیر هستند:

- مسیر ارتباطی با استفاده از کانال‌های ارتباطی داخلی و خارجی ایجاد شده است که زیر مجموعه مشخصی از داده توابع امنیتی هدف ارزیابی و دستورات را از باقی توابع امنیتی هدف ارزیابی و داده کاربر جدا می‌کند.
- استفاده از مسیر ارتباطی ممکن توسط کاربر و یا توابع امنیتی هدف ارزیابی آغاز شود.
- مسیر ارتباطی می‌تواند اطمینان دهد که کاربر با توابع امنیتی هدف ارزیابی به طور صحیح در ارتباط است و اینکه توابع امنیتی هدف ارزیابی با کاربر به طور صحیح

در ارتباط است.

در این نمونه، یک کانال امن، کانال ارتباطی است که ممکن است از هر دو سوی کانال راه‌اندازی شود و ارائه دهنده‌ی شاخصه‌ی غیرقابل انکار بودن با توجه به هویت آن سمت از کانال است.

یک مسیر امن، ارائه دهنده قابلیتی برای کاربران است تا فعالیتشان را از طریق یک تعامل مستقیم و مطمئن یا توابع امنیتی هدف ارزیابی انجام دهند. مسیر امن غالباً برای اقدامات کاربر هم‌چون شناسایی و احراز هویت اولیه مطلوب است، اما ممکن است در زمان‌های دیگری در طول بازه زمانی یک نشست کاربری نیز مفید باشد و تبادلات مسیر امن ممکن است توسط کاربر یا توابع امنیتی هدف ارزیابی آغاز شود. پاسخ امن از طریق مسیر امن تضمین می‌کند که از تغییرات توسط برنامه ناامن یا افشاء شدن برای یک برنامه ناامن محافظت می‌کند.

- **کانال مورداعتماد بین توابع امنیتی هدف ارزیابی[1]**

این خانواده تعریف کننده الزاماتی برای ایجاد یک کانال ارتباطی امن بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT است تا عملکردهای حساس امنیتی کارایی لازم را داشته باشد. این خانواده باید هنگامی‌که الزاماتی برای ارتباط امن کاربر یا داده توابع امنیتی هدف ارزیابی بین هدف ارزیابی و دیگر محصولات امن IT وجود دارد، در نظر گرفته شود.

- **مسیر مورداعتماد[2]**

1 Inter-TSF trusted channel(FTP_ITC)

2 Trusted path(FTP_TRP)

این خانواده تعریف کننده الزاماتی برای برقراری و نگهداری ارتباط امن به/از کاربران و توابع امنیتی هدف ارزیابی است. یک مسیر امن ممکن است برای هر تعامل مرتبط امنیتی لازم باشد. تبادلات مسیر امن ممکن است توسط کاربر در طول تعامل با توابع امنیتی هدف ارزیابی آغاز شود، یا توابع امنیتی هدف ارزیابی ممکن است از طریق مسیر امن، ارتباطی را با کاربر برقرار کنند.

شماره الزام	نام خانواده	عنصر امنیتی
۱۰۲	کانال مطمئن داخلی توابع امنیتی هدف ارزیابی (FTP_ITC)	**نام عنصر: کانال مطمئن داخلی توابع امنیتی هدف ارزیابی(جلوگیری از افشاء) ۱** **شماره مؤلفه: مم-ک‌م.۱،۱(FTP_ITC.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید کانالی ارتباطی امنی با استفاده از [انتخاب: IPsec، SSH، TLS، TLS/HTTPS] میان خود و سایر محصولات فناوری اطلاعات مطمئن فراهم کندکه از قابلیت‌های زیر پشتیبانی می‌کنند: سرور ممیزی[انتخاب: سرور احراز هویت،[اختصاص: دیگر قابلیت‌ها]] که به طور منطقی از سایر کانال‌های ارتباطی جدا است و به صورت مطمئن نقطه پایانی‌اش را شناسایی می‌کند و از داده‌های کانال در برابر تغییر یا افشاء، محافظت کند.
۱۰۳		**نام عنصر: کانال مطمئن داخلی توابع امنیتی هدف ارزیابی ۱**

شماره	نام خانواده	عنصر امنیتی
الزام		

شماره مؤلفه: مم-ک‌م.۲,۱(FTP_ITC.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اجازه شروع ارتباط از طریق کانال مطمئن را به خود و سایر محصولات فناوری اطلاعات مطمئن بدهد.

۱۰۴ **نام عنصر: کانال مطمئن داخلی توابع امنیتی هدف ارزیابی ۱**

شماره مؤلفه: مم-ک‌م.۳,۱(FTP_ITC.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید ارتباطات را از طریق کانال مطمئن برای [اختصاص: لیستی از سرویس‌هایی که توابع امنیتی هدف ارزیابی که قادر به شروع ارتباط هستند] شروع کند.

نکته کاربردی:

منظور الزام بالا استفاده از پروتکل رمزنگاری، جهت محافظت از ارتباطات خارجی با محصولات فناوری اطلاعات مطمئن است که با هدف ارزیابی یا اجرای عملکردشان در تعامل هستند. برای ارتباطات با سروری که اطلاعات ممیزی را جمع‌آوری می‌کند، محافظت از ارتباط توسط یکی از پروتکل‌های لیست شده در بالا، لازم و ضروری می‌باشد. اگر ارتباطی با یک سرور احراز هویت برقرار شده باشد (به عنوان

شماره نام خانواده

عنصر امنیتی

الزام

مثال RADIUS)، بنابراین نویسنده هدف امنیتی در مؤلفه مم-کم.۱,۱ «سرور احراز هویت» را انتخاب می‌کند و این اتصال باید توسط یکی از پروتکل‌های لیست شده محافظت شود. چنان‌چه دیگر محصولات فناوری اطلاعات مطمئن (همانند سرور NTP) محافظت شوند، نویسنده هدف امنیتی اختصاص(برای آن محصول) و انتخاب(برای پروتکل‌هایی که جهت محافظت از ارتباطات استفاده می‌شوند) مناسبی را انجام می‌دهد. پس از آنکه نویسنده هدف امنیتی انتخاب‌هایش را انجام داد، نویسنده باید با توجه به پیوست جزئیات الزامات مربوط به پروتکل را در متن هدف امنیتی قرار دهد.

به طور خلاصه، اتصال به یک سرور جمع‌آوری کننده ممیزی خارجی لازم است توسط یکی از پروتکل‌های لیست شده محافظت شود. اگر یک سرور احراز هویت کننده خارجی محافظت می‌شود، بنابراین نیاز به محافظت اتصالش با یکی از پروتکل‌های لیست شده است. برای هر سرور خارجی دیگر، لازم به حفاظت اتصالات خارجی نیست. اما اگر ادعای حفاظت مطرح شود، باید با یکی از پروتکل‌های شناخته شده محافظت شوند.

درحالیکه هیچ الزام دیگری برای شروع ارتباطات وجود ندارد، نویسنده هدف امنیتی در قسمت «اختصاص» مؤلفه مم-کم.۳,۱ سرویس-هایی را لیست می‌کند که هدف ارزیابی بتواند ارتباطش را به محصولات فن‌آوری اطلاعات مطمئن شروع کند.

این الزام نشان می‌دهد که ارتباط محافظت شده نه تنها در زمان برقراری ارتباط ایجاد می‌شود، هم‌چنین پس از قطعی ارتباط دوباره از

شماره	نام خانواده	عنصر امنیتی
	الزام	

سر گرفته می‌شود. در مواردی که بخشی از تنظیمات هدف ارزیابی، به صورت دستی تونل‌ها را جهت حفاظت ارتباطات دیگر راه‌اندازی می‌کند و چنان‌چه پس از قطعی ارتباط، هدف ارزیابی سعی در برقراری مجدد ارتباط به صورت خودکار یا مداخله دستی می‌کند ممکن است فرصتی ایجاد شود که مهاجم قادر به دستیابی به اطلاعات بحرانی شود یا اتصال به خطر افتد.

۱۰۵ مسیر مطمئن (FTP_TRP)

نام عنصر: مسیر مطمئن ۱

شماره مؤلفه:م‌م-م‌م.۱,۱(FTP_TRP.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید مسیر ارتباطی امنی با استفاده از [انتخاب، انتخاب حداقل یکی از: IPsec، SSH، TLS، TLS/HTTPS] میان خود و سرپرست از راه دور فراهم کند که به صورت منطقی از دیگر مسیرهای ارتباطی مجزا می‌باشد و نقاط پایانی[1] خود را به صورت مطمئن شناسایی و از داده‌های تبادلی در برابر تغییر، افشاء، ، محافظت می‌کند و تغییرات داده‌های تبادلی را مشخص می‌کند.

۱۰۶

نام عنصر: مسیر مطمئن ۱

شماره مؤلفه:م‌م-م‌م.۱,۲(FTP_TRP.1.2)

1 End points

شماره	نام خانواده	عنصر امنیتی
	الزام	

شرح مؤلفه:

توابع امنیتی هدف ارزیابی به سرپرست از راه دور، اجازه ایجاد ارتباط از طریق مسیر مطمئن را بدهند.

۱۰۷ **نام عنصر: مسیر مطمئن ۱**

شماره مؤلفه:م‌م-م‌م.۱,۳(FTP_TRP.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید از مسیر مطمئنی برای احراز هویت اولیه سرپرست یا تمام اقدامات سرپرستی از راه دور استفاده کنند.

نکته کاربردی:

این الزام اطمینان می‌دهد که سرپرستان از راه دور تمام ارتباطاتشان را با هدف ارزیابی از طریق یک مسیر امن شروع می‌کنند و تمام ارتباطات با هدف ارزیابی توسط سرپرستان از راه دور بر روی این مسیر انجام می‌گیرد. داده منتقل شده در این کانال ارتباطی امن توسط پروتکلی که در «انتخاب» اول برگزیده شده است، رمز می‌شود. نویسنده هدف امنیتی سازوکار یا سازوکارهای پشتیبانی شده توسط هدف ارزیابی را انتخاب می‌کند و این اطمینان را می‌دهد که جزئیات الزام در پیوست C به متن هدف امنیتی کپی می‌شود.

۸ کلاس توسعه

نام کلاس	نام کامپوننت	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری عملیاتی
	AGD_PRE.1	راهنمای کاربری آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل- انطباق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش مدیریت پیکربندی هدف ارزیابی

۸,۱ مشخصات کارکردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱۰۸	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: توسعه دهنده باید مشخصات کارکردی را ارائه کند.
۱۰۹		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده-سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات هدف ارزیابی» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات هدف ارزیابی» وجود داشته باشند،

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		الزامات کارکردی تضمین می‌شوند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۱۱۰	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مشخصات کارکردی باید اهداف و روش‌های مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [1] و پشتیبان کننده‌ی الزام کارکرد امنیتی [2] توصیف کند.
۱۱۱		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص کند.
۱۱۲		**نام عنصر: مشخصات کارکرد ابتدایی۱**

1 SFR-enforcing TSFI

2 SFR-supporting TSFI

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (ADV_FSP.1.3C) **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه کند.
۱۱۳		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب

شماره الزام	نام خانواده	عنصر امنیتی
۱۱۴	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.
۱۱۵		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** ارزیاب باید مشخص کند که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می-باشند.

۸,۲ کلاس راهنمای کاربر

۸,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه دهنده

شماره الزام	نام خانواده	عنصر امنیتی
۱۱۶	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۱۷	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی که باید در یک محیط پردازشی امن کنترل شوند را توصیف کند، همانند هشدارهای مناسب.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۱۱۸		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسطهای در دسترس ارائه شده توسط هدف ارزیابی به صورت امن استفاده می‌شود.
۱۱۹		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطهای دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین کند.
۱۲۰		**نام عنصر: راهنمای کاربردی ۱**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (AGD_OPE.1.4C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط کند، همانند تغییر مشخصات امنیتی موجودیت-های تحت کنترل توابع امنیتی هدف ارزیابی.
۱۲۱		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مودهای عملیاتی هدف ارزیابی (مودهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
۱۲۲		**نام عنصر: راهنمای کاربردی ۱**

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

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی

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

۸,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱۲۵	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		توسعه دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۲۶	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن هدف ارزیابی توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح نمایند.
۱۲۷		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2C)**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن هدف ارزیابی و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح نمایند.

مؤلفه‌های اقدامات ارزیاب		
۱۲۸	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۱۲۹		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
		ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید کند، هدف ارزیابی می‌تواند به صورت امن برای عمل نمودن آماده شود.

۸,۳ کلاس آزمون

آزمون هدف ارزیابی برای بررسی کارکرد سیستم و جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند، در نظر گرفته می‌شود. آزمون کارکردی سیستم از طریق خانواده ATE_IND و آزمون جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون براساس کارکردی که برای هدف ارزیابی در نظر گرفته شده و واسطهایی که بر اساس اطلاعات طراحی در اختیار قرار می‌گیرند، انجام می‌شود. یکی از خروجی‌های اولیه پروسه ارزیابی گزارش آزمون می‌باشد که در الزامات زیر مشخص شده است.

۸,۳,۱ آزمون مستقل

این دسته از آزمون‌ها برای تائید عملکردی که در بخش «مشخصات امنیتی هدف ارزیابی» و مستندات سرپرستی ارائه شده است، صورت می‌گیرند. تمرکز آزمون‌ها بر روی برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. فعالیت‌های تضمین حداقل آزمون‌های مربوط به این بخش‌ها را معرفی می‌کند و ارزیاب گزارشی از طرح آزمون و نتایج آن آماده می‌کند.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**

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

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

مؤلفه‌های اقدامات ارزیاب		
۱۳۲	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌کند.
۱۳۳		**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را بیازماید تا تائید کند که توابع امنیتی هدف ارزیابی به صورت مشخص شده عمل می‌کنند.

۸,۴ کلاس آسیب‌پذیری

برای آماده نمودن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی آن دسته از آسیب‌پذیری‌هایی که در این نوع محصولات یافت شده-اند بیابد. غالباً سوء استفاده از این آسیب‌پذیری‌ها(یافتن آسیب‌پذیری‌های در آزمایشگاه) نیاز به مهارت و تخصص مهاجمان دارد.
تا زمانی‌که ابزارهای نفوذ در تمام آزمایشگاه‌ها توزیع می‌شوند و در دسترس هستند، انتظار نمی‌رود که ارزیاب‌ها برای این دسته از آسیب‌پذیری‌های هدف ارزیابی را مورد آزمون قرار دهند. آزمایشگاه‌ها انتظار دارند توضیحاتی پیرامون احتمال کلی این دسته از آسیب‌پذیری‌ها در مستنداتی که توسط فروشنده به کاربران ارائه می‌شود لحاظ شود. اینگونه اطلاعات در توسعه ابزارهای آزمون نفوذ و همچنین نسخه‌های بعدی پروفایل‌های حفاظتی مورد استفاده قرار خواهند گرفت.

۸,۴,۱ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۳۴	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمودن، هدف ارزیابی را ارائه کند.

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

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۱۳۶	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌کند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۱۳۷		**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد.
۱۳۸		**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ را انجام دهد تا مقاومت هدف ارزیابی در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص کند.

۸,۵ کلاس پشتیبانی از چرخه حیات

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

۸,۵,۱ قابلیت‌های پیکربندی

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

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

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

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۴۱	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۸,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱۴۲	حوزه پیکربندی (ALC_CMS)	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه کند.

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

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۱۴۴		**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی کند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۱۴۵	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند..

۹ پیوست الف

همان‌گونه که در این پروفایل حفاظتی نشان داده شده است، چندین روش وجود دارد که هدف ارزیابی منطبق بر این پروفایل حفاظتی، می‌تواند تهدیدهای مرتبط با به خطر افتادن کانال ارتباطی بین سرپرستان و دیگر بخش‌های هدف ارزیابی یا موجودیت‌های IT خارجی را کاهش دهد. یکی از پروتکل‌های ارتباطی امن (IPSECT، SSHT، TLS، TLS/HTTPS) باید پیاده‌سازی شود تا اتصال محافظت شده‌ای برای سرور ممیزی و سرپرستان راه دور فراهم آورد. از آنجایی که الزامات مرتبط با هریک از پروتکل‌ها وجود دارد، مشخص کردن پروتکل‌ها در این پروفایل حفاظتی مبهم و مشکل ساز می‌شود، از این‌رو مشخص کردن الزامات اختیاری توسط استاندارد معیار مشترک پشتیبانی نمی‌شود. با توجه به انتخاب عناصر مم-مم.۱ و مم-ک‌م.۱ ، الزامات زیر نیز باید در سند هدف امنیتی نیز در نظر گرفته شود.

علاوه براین، هدف‌های ارزیابی توزیعی، مجاز هستند که ادعای انطباق با این پروفایل حفاظتی را داشته باشند. در این موارد، نیاز است که ارتباط مابین بخش‌های مختلف هدف ارزیابی محافظت شود و هم‌چنین نویسنده هدف امنیتی باید دو تکرار خانواده حت-اد در بدنه اصلی هدف امنیتی در نظر بگیرد.

توجه شود که تنظیم جزئی اطلاعات روایی در شروع هدف امنیتی با توجه به انتخاب‌های انجام شده، ممکن است لازم باشد. علاوه براین، با توجه به الزامات انتخاب شده، لازم است اطلاعات مناسبی توسط بخش الف۲,۱ رویدادهای قابل ممیزی به جدول رویدادهای قابل ممیزی در هدف امنیتی اضافه شود.

۹,۱ الزامات

شماره الزام	نام خانواده	عنصر امنیتی
۱۴۶	رز-اپ-(ت‌س)	نام عنصر: پروتکل IPSEC ۱ شماره مؤلفه: رز-اپ-(ت‌س).۱,۱ FCS_IPSEC_EX

شماره	نام خانواده	عنصر امنیتی
الزام		
T.1 Explicit: IPSEC		

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید ESP[1] پروتکل IPsec را به صورت تعریف شده توسط RFC4303 و با استفاده از الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-256(هردوی اینها توسط RFC 3602 مشخص شده است)، [انتخاب: هیچ الگوریتم دیگر، AES-GCM-128، AES-GCM-256 مشخص شده در RFC 4106]، و بااستفاده از [انتخاب، حداقل یکی از موارد: IKEv1 به صورت تعریف شده در RFC 2407، 2408، 2409، RFC 4109، و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]؛ IKEv2 در RFC 5996 تعریف شده است، 4307، و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]] پیاده‌سازی کنند.

نکته کاربردی:

اولین انتخاب به این جهت استفاده می‌شود تا الگوریتم‌های رمزنگاری اضافی را که پشتیبانی می‌شوند معرفی کند. در دومین انتخاب باید پشتیبانی از IKEv1 و یا IKEv2 صورت گیرد، هرچند هدف ارزیابی ممکن است بر هردو منطبق باشد.

برای IKEv1، الزام تفسیر می‌شود در صورتی که پیاده‌سازی IKE مطابق با RFC 2409 باشد و اضافات

1 Encapsulating Security Payload

شماره	نام خانواده	عنصر امنیتی
الزام		
		و تغییرات در RFC 4109 توصیف شده باشد. RFC 4868 توابع درهم‌سازی اضافی را برای استفاده IKEv1 و IKEv2 معرفی می‌کند. چنان‌چه این توابع پیاده‌سازی شوند، سومین (برای IKEv1) و چهارمین (IKEv2) انتخاب می‌تواند استفاده شود.
۱۴۷		**نام عنصر: پروتکل IPSEC ۱** **شماره مؤلفه: رز-اپ-(ت‌س).۲,۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید این اطمینان را بدهد که تبادلات فاز ۱ IKEv1 تنها در مود اصلی استفاده می‌شود.
۱۴۸		**نام عنصر: پروتکل IPSEC ۱** **شماره مؤلفه: رز-اپ-(ت‌س).۳,۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اطمینان دهد که طول عمر SA مربوط به IKEv1 قادر است برای فاز ۱ SA به ۲۴ ساعت محدود شود و برای فاز ۲ SA به ۸ ساعت محدود شود.

شماره نام خانواده
الزام

عنصر امنیتی

نکته کاربردی:

الزام بالا می‌تواند توسط طول عمری که توسط سرپرست امنیتی قابل تنظیم است (با الزامات FMT مناسب، یا دستورات ذکر شده در سندی که در AGD_OPE مطرح شده است) یا توسط «کدنویسی سخت» که پیاده‌سازی را محدود می‌کند انجام شود.

۱۴۹

نام عنصر: پروتکل IPSEC ۱

شماره مؤلفه: رز-اپ-(ت‌س).۴,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد که طول عمر SA مربوط به IKEv1 قادر است برای فاز ۲ SA به [اختصاص: عددی بین ۱۰۰-۲۰۰] مگابایت، محدود شود.

نکته کاربردی:

الزام بالا می‌تواند توسط طول عمری که توسط سرپرست امنیتی قابل تنظیم است (با الزامات FMT مناسب، یا دستورات ذکر شده در سندی که در AGD_OPE مطرح شده است) یا توسط « کدنویسی سخت» که پیاده‌سازی را محدود می‌کند، انجام شود. نویسنده هدف امنیتی، مقدار عددی را در بازه مشخص شده تعیین می‌کند.

شماره	نام خانواده الزام	عنصر امنیتی

به طورکلی، دستورالعمل‌ها برای تنظیم پارامترهای پیاده‌سازی، هم‌چون طول عمر SA، باید توسط الزامات FMT مشخص شود و در راهنماهای سرپرستی که برای الزام AGD_OPE تولید شده، نیز ذکر شده باشد.

۱۵۰

نام عنصر: پروتکل IPSEC ۱

شماره مؤلفه: رز-اپ-(ت‌س).۵,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد که تمام پروتکل‌های IKE گروه‌های DH، ۱۴(۲۰۴۸ بیت MODP)، و [انتخاب: ۲۴(۲۰۴۸ بیت MODP با ۲۵۶ بیت POS)، ۱۹ (۲۵۶ بیت تصادفی ECP)، ۲۰ (۳۸۴ بیت تصادفی ECP)، [اختصاص: دیگر گروه‌های DH که توسط هدف ارزیابی پیاده‌سازی شده‌اند]، هیچ گروه دیگر DH] را پیاده‌سازی می‌کنند.

نکته کاربردی:

این مؤلفه هدف ارزیابی را ملزم به پشتیبانی از گروه DH 14 می‌کند. در صورت پشتیبانی از دیگر گروه-ها، این گروه‌ها باید انتخاب شوند یا در قسمت «اختصاص» بالا مشخص شوند، در غیر این‌صورت «هیچ گروه دیگر DH » انتخاب می‌شود. این الزام به تبادلات IKEv1 و (در صورت پیاده‌سازی) به IKEv2

شماره	نام خانواده	عنصر امنیتی
	الزام	
		اعمال می‌شود.
۱۵۱		**نام عنصر: پروتکل IPSEC ۱** **شماره مؤلفه: رز-اپ-(ت‌س).۶,۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اطمینان دهد که تمام پروتکل‌های IKE با استفاده از الگوریتم [انتخاب: DSA، rDSA، ECDSA] احراز هویت را پیاده‌سازی می‌کند. **نکته کاربردی:** الگوریتم انتخاب شده باید با انتخاب صورت گرفته در مؤلفه رز-ع‌ر.۱(۲) در ارتباط باشد.
۱۵۲		**نام عنصر: پروتکل IPSEC ۱** **شماره مؤلفه: رز-اپ-(ت‌س).۷,۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید استفاده‌ی کلیدهای از قبل به اشتراک گذاشته شده را (همان‌طور که در

شماره نام خانواده

الزام

عنصر امنیتی

RFC ها اشاره شده است) برای استفاده در احراز هویت اتصالات خود IPsec پشتیبانی کند.

۱۵۳

نام عنصر: پروتکل IPSEC ۱

شماره مؤلفه: رز-اپ-(ت‌س).۸,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید موارد زیر را پشتیبانی کند:

- کلیدهای از پیش به اشتراک گذارده شده، باید قادر باشند از هرترکیبی از حروف بزرگ، حروف کوچک، اعداد و کاراکترهای خاص: [انتخاب: "!"، "@"، "#"، "$"،"٪"،"^"،"&"،"*"،")"،"(", [اختصاص: دیگر کاراکترها]] تشکیل شوند.
- کلیدهای از پیش به اشتراک گذاشته شده ۲۲ کاراکتر و [انتخاب: [اختصاص: دیگر طول کلیدهایی که پشتیبانی می‌شود]، بدون دیگر اندازه‌های کلید] باشد.

نکته کاربردی:

نویسنده هدف امنیتی باید کاراکترهای خاصی را انتخاب کند که توسط هدف ارزیابی قابل پشتیبانی باشد. ممکن است با استفاده از قابلیتی که در قسمت «اختصاص» ارائه شده، این اختیار به نویسنده داده

شماره الزام	نام خانواده عنصر امنیتی
	شده است تا بتواند کاراکترهای بیشتری را تعریف کند. برای طول کلیدهای از پیش به اشتراک گذاشته شده، طول کلید معمولی (۲۲ کاراکتر) برای کمک به ترویج قابلیت همکاری نیاز است. اگر طول کلیدهای دیگر پشتیبانی می‌شود باید در قسمت "اختصاص" لیست شود، هم‌چنین در این قسمت می‌توان یک محدوده را برای طول کلید مشخص نمود(به طور مثال طول کلید از ۵ تا ۵۵ کاراکتر).

شماره الزام	نام خانواده عنصر امنیتی
۱۵۴ رز-ل‌ا-(ت‌س).۱ FCS_TLS_EXT.1 Explicit: TLS	**نام عنصر: پروتکل TLS ۱** **شماره مؤلفه: رز-ل‌ا-(ت‌س).۱,۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید یک یا بیش از یکی از پروتکل‌های زیر را [انتخاب: TLS 1.0 (RFC 2246)، TLS 1.1 (RFC 4364)، TLS 1.2 (RFC 5264)] پیاده‌سازی کند که از دنباله‌های رمز زیر پشتیبانی می‌کند: **دنباله رمز الزامی:**

شماره	نام خانواده	عنصر امنیتی
		الزام

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

دنباله رمز اختیاری:

[انتخاب:

هیچکدام

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

شماره الزام	نام خانواده	عنصر امنیتی
		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

نکته کاربردی:

نویسنده هدف امنیتی باید در این مؤلفه اختصاص و انتخاب مناسبی داشته باشد تا پیاده‌سازی TLS را منعکس کند. نویسنده هدف امنیتی باید جزئیات کافی ارائه دهد تا بتواند مشخص کند که کدام پیاده-سازی منطبق بر استانداردهای معرفی شده است، این امر می‌تواند توسط اضافه کردن مؤلفه ها به این عنصر یا با اضافه کردن جزئیات به TSS صورت گیرد.

دنباله رمز، در پیکربندی‌های ارزیابی شده‌ای که توسط این الزام محدود شده‌اند استفاده می‌شود. نویسنده هدف امنیتی باید دنباله‌های رمز اختیاری را که پشتیبانی می‌شوند انتخاب کند؛ اگر به غیر از دنباله‌های اجباری، دنباله رمزی جهت پشتیبانی وجود نداشته باشد، «هیچ‌کدام» باید انتخاب شود*****

۱۵۵

رز-پ‌ا-(ت‌س).۱ **نام عنصر: پروتکل SSH ۱**

FCS_SSH_EXT.1

Explicit: SSH

شماره مؤلفه: رز-پ‌ا-(ت‌س).۱,۱

شرح مؤلفه:

شماره	نام خانواده	عنصر امنیتی
الزام		
		توابع امنیتی هدف ارزیابی باید پروتکل SSH را منطبق بر RFC 4251، 4252، 4253 و 4254 پیاده-سازی کند.
		نکته کاربردی:
		نویسنده هدف امنیتی باید جزئیات کافی ارائه دهد تا مشخص کند که چگونه پیاده‌سازی بر استانداردهای معرفی شده منطبق است، این امر می‌تواند با اضافه کردن مؤلفه‌ها به این عنصر و یا با اضافه کردن جزئیات در TSS صورت گیرد.
۱۵۶		**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-پ‌ا-(ت‌س).۲,۱
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اطمینان دهد که پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر را که در RFC 4253 توصیف شده است پشتیبانی می‌کند: مبتنی بر کلید عمومی، مبتنی بر پسورد.
۱۵۷		**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-پ‌ا-(ت‌س).۳,۱

شماره نام خانواده
الزام

عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد همان‌طور که در RFC 4253 توصیف شده است، بسته‌های بزرگتر از [اختصاص: عددی برای مشخص کردن بایت] بایت در اتصال انتقال SSH حذف می‌شوند.

نکته کاربردی:

RFC 4253 برای پذیرش «بسته‌های بزرگ» ارائه شده است، و هشدار می‌دهد که اندازه بسته باید یک «اندازه منطقی» باشد در غیر این صورت بسته حذف می‌شودد. قسمت «اختصاص» باید توسط نویسنده هدف امنیتی با حداکثر اندازه بسته که پذیرفته می‌شود کامل شود، بنابراین «اندازه منطقی‌ای» برای هدف ارزیابی تعریف می‌شود.

۱۵۸

نام عنصر: پروتکل SSH ۱

شماره مؤلفه: رز-پا-(ت‌س).۴,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد، پیاده‌سازی انتقال SSH از الگوریتم‌های رمزنگاری زیر استفاده می‌کند: AES-CBC-128، AES-CBC-256، [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، بدون هیچ الگوریتم دیگر].

شماره نام خانواده
الزام

عنصر امنیتی

نکته کاربردی:

در قسمت «اختصاص» نویسنده هدف امنیتی می‌تواند الگوریتم‌های AES-GCM انتخاب کند یا در صورتی‌که از الگوریتم AES-GCM پشتیبانی نمی‌کند، «بدون هیچ الگوریتم دیگر» انتخاب می‌شود.

در صورت انتخاب AES-GCM باید ارتباطاتی در سراسرخانواده رز-ع‌ر در هدف امنیتی وجود داشته باشد. ***

۱۵۹

نام عنصر: پروتکل SSH ۱

شماره مؤلفه: رز-پ‌ا-(ت‌س).۵,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد، پیاده‌سازی انتقال SSH از الگوریتم‌های کلید عمومی زیر استفاده می‌کند: SSH_RSA، [انتخاب: PGP-Sign-RSA، PGP-Sign-RSA ، بدون هیچ الگوریتم دیگر].

نکته کاربردی:

RFC 4253 الگوریتم‌های کلید عمومی مجاز و ضروری را مشخص کرده است. این الزام سبب ضروری

شماره	نام خانواده	عنصر امنیتی
الزام		
		شدن SSH-RSA می‌شود و به PGP-Sign-RSA،PGP-Sign-RSA اجازه می‌دهد تا در هدف امنیتی، ادعا شود. نویسنده هدف امنیتی باید انتخاب مناسبی داشته باشد و در صورتی‌که تنها SSH_RSA پیاده‌سازی شده باشد «بدون هیچ الگوریتم عمومی» انتخاب می‌شود.
۱۶۰		**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-پا-(ت‌س).۶,۱
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اطمینان دهد، الگوریتم‌های یکپارچگی داده در اتصال انتقال SSH که یک [انتخاب: hmac-sha1، hmac-sha1-96، hmac-md5، hmac-md5-96] است استفاده می‌شود.
۱۶۱		**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-پا-(ت‌س).۷,۱
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اطمینان دهد که diffie-hellman-group14-sha1 تنها به روش‌های

شماره	نام خانواده	عنصر امنیتی
الزام		
		تبادل کلید اجازه می‌دهد تا برای پروتکل SSH استفاده شود.

شماره	نام خانواده	عنصر امنیتی
الزام		
۱۶۲	رز-اف-(ت‌س).۱ FCS_HTTPS_EXT.1 Explicit: HTTPS	**نام عنصر: پروتکل HTTPS ۱** **شماره مؤلفه: رز-اف-(ت‌س).۱,۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 پیاده‌سازی کند. **نکته کاربردی:** نویسنده هدف امنیتی باید جزئیات کافی را ارائه دهد تا مشخص کند چگونه پیاده‌سازی با استاندارد معرفی شده مطابقت دارد، این امر می‌تواند با اضافه کردن مؤلفه‌ها به عنصر یا با اضافه کردن جزئیات TSS صورت گیرد.
۱۶۳		**نام عنصر: پروتکل HTTPS ۱**

شماره الزام	نام خانواده	عنصر امنیتی

شماره مؤلفه: رز-اف-(ت‌س).۲,۱.

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید HTTPS را با استفاده از TLS به صورت مشخص شده در رز-ل‌ا-(ت-س).۱ پیاده‌سازی کند.

۱۶۴ **حت-اد (FPT-ITT)** **نام عنصر: انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی ۱**

شماره مؤلفه: حت-اد-(ت‌س).۱,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید داده‌اش را از افشاء محافظت کند و تغییراتش را زمانی‌که بین بخش‌های مجزای هدف ارزیابی از طریق استفاده از [انتخاب حداقل یکی از: IPsec، SSH، TLS، TLS/HTTPS] انتقال می‌یابد تشخیص دهد .

نکته کاربردی:

این الزام اطمینان می‌دهد که تمام ارتباطات بین عناصر هدف ارزیابی توسعه یافته، با استفاده از یک کانال ارتباطی رمز شده محافظت می‌شود. داده‌های منتقل شده در این کانال ارتباطی، توسط پروتکلی

شماره	نام خانواده	عنصر امنیتی
الزام		
		که در انتخاب اول مشخص شده است، رمز می‌شود. نویسنده هدف امنیتی سازوکار یـا سـازوکارهـایی را انتخاب می‌کند که توسط هدف ارزیابی پشتیبانی شود و این اطمینان را می‌دهد که جزئیات الزام در این پیوست مربوط به انتخابی که کرده‌اند (توسط نویسنده هدف امنیتی) در صورتی‌که در سند هدف امنیتی وجود نداشته باشد، به آن کپی می‌شود.

۹,۲ رویداد قابل ممیزی

با توجه به الزامات خاصی که توسط نویسنده هدف امنیتی در قسمت ۹,۱ انتخاب شده است، نویسنده هدف امنیتی باید رویدادهای قابل ممیزی مناسبی را در جدول مربوطه در هدف امنیتی، برای الزامات انتخاب شده در نظر بگیرد.

محتوای رکورد ممیزی اضافی	رویدادهای قابل ممیزی	الزام
علت خرابی نقطه پایانی اتصال غیرهدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی	خرابی در ایجاد SA مربوط به IPsec ایجاد و خاتمه دادن SA مربوط به IPsec	رز-اپ-(ت‌س).۱ FCS_IPSEC_EXT.1

علت خرابی نقطه پایانی اتصال غیر-هدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی	خرابی در ایجاد یک نشست TLS برقراری/خاتمه نشست TLS	رز-ل‌ا-(ت‌س).۱ FCS_TLS_EXT.1
علت خرابی نقطه پایانی اتصال غیرهدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی	خرابی در ایجاد یک نشست SSH برقراری/خاتمه نشست SSH	رز-پ‌ا-(ت‌س).۱ FCS_SSH_EXT.1
علت خرابی نقطه پایانی اتصال غیرهدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی	خرابی در ایجاد نشست HTTPS برقراری/خاتمه نشست HTTPS	رز-اف-(ت‌س).۱ FCS_HTTPS_EXT.1
هیچکدام	هیچکدام	حت-اد.۱(۱) FPT_ITT.1(1)

هیچکدام	هیچکدام	حت-اد.۱(۲) FPT_ITT.1(2)