به نام خدا

پروفایل حفاظتی VPN Client

نسخه ۱,۶

اردیبهشت 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 VPN client می‌باشد تا تولیدکنندگان این دسته از محصولات بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ و همچنین سند هدف امنیتی آن را ارائه کنند.

در بخش اول VPN client به صورت کلی معرفی 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 VPN client در این سند مطرح شده است عبارتند از:

- کلاس پشتیبانی از رمزنگاری
- کلاس حفاظت از داده‌های کاربری
- کلاس شناسایی و احراز هویت
- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی

- کلاس کانال/ مسیر امن

هر کلاس مجموعه‌ای از خانواده و هر خانواده مجموعه‌ای از مولفه و هر مولفه مجموعه‌ای از عناصر می‌باشد. با استفاده از «الزامات کارکرد امنیتی» در واقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌گردد.

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

فهرست

۱ هدف از ارائه سند

در راستای ارزیابی امنیتی محصولات مبتنی بر 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 را که در این سند برای برآورده کردن الزامات ارائه شده‌اند در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

۲ معرفی اصطلاحات

- **هدف ارزیابی (TOE)**

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

- **پروفایل حفاظتی (PP[1])**

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

1 Protection Profile

- **هدف امنیتی (ST[1])**

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.

- **غیر هدف ارزیابی (Non-TOE[2])**

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.

- **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.

---

1 Security Target

2 Non-Target Of Evaluation

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

- **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 مجموعه-ای 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 تهدیدهای 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 کنند.

[1] Organizational Security Policy

- **الزام کارکرد امنیتی(SFR[1])**

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

- **الزامات تضمین امنیتی (SAR[2])**

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[3])**

[1] Security Functional Requirement

[2] Security Assurance Requirement

[3] Evaluation Assurance Level

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

- **توابع امنیتی هدف ارزیابی (TSFs[1])**

آن بخش از هدف ارزیابی که برای اجرای صحیح «الزامات کارکرد امنیتی» باید به آن تکیه کرد، 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 کرد.

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

داده‌هایی برای عملیات هدف ارزیابی هستند که اجرای الزامات کارکرد امنیتی وابسته به آنها است. 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 تأثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به کار برده می‌شوند. محتویات پیام الکترونیکی نوعی داده کاربری می‌باشد.

1 TOE Security Functions

- **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.

- **اختصاص (Assignment)**

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

- **انتخاب (Selection)**

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

---

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

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

- **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) است که شامل اطلاعات است و یا اطلاعات را دریافت می‌کند و روی آن توسط موجودیت-های فعال، عملیاتی انجام می‌گیرد. همانند داده ها و اطلاعاتی همچون متن های 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.

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

1 Security Functionality Policy

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» سازوکارهایی 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 کنند.

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

«خط‌مشی جریان اطلاعات» سازوکارهایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی-شان 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 مولفه‌های عملکرد امنیتی بوده که مبنایی برای ارزیابی الزامات عملکرد امنیتی موجود در پروفایل حفاظتی[2]یا هدف امنیتی[3]است.

این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[4]یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده نمودن اهداف امنیتی که در پروفایل حفاظتی یا هدف امنیتی تعیین شده است، 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 [5]

بخش سوم: الزامات تضمین امنیتی [1]

---

[1] Common Criteria (CC)

[2] Protection Profile (PP)

[3] Security Target (ST)

[4] Target Of Evaluation (TOE)

[5] Security Functional Requirement (SFR)

۴ معرفی VPN client

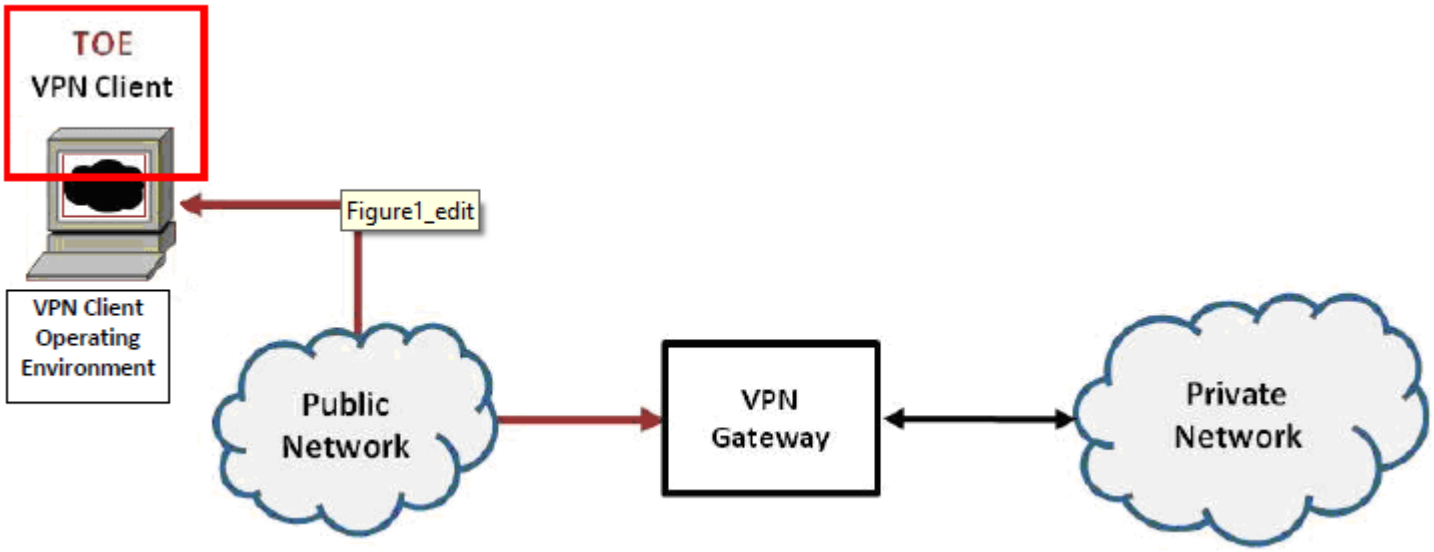
این پروفایل حفاظتی مشخص کننده‌ی الزامات عملکرد امنیتی برای کلاینت VPN می‌باشد. VPN، داده‌های خصوصی را به صورت محافظت شده بین کلاینت‌های VPN و دروازه‌های VPN منتقل می‌کند. هدف ارزیابی تعریف شده در این پروفایل حفاظتی کلاینت VPN می‌باشد که بر روی کلاینت دسترسی راه دور اجرا می‌شود. کلاینتVPN در نظرگرفته شده در داخل و یا خارج از شبکه خصوصی قرار می‌گیرد و یک تونل امن به دروازه VPN فراهم می‌آورد. این تونل برای اطلاعاتی که در شبکه عمومی در گردش است محرمانگی، یکپارچگی و احراز هویت داده را فراهم می‌کند. تمام کلاینت‌های VPN که منطبق بر این پروفایل حفاظتی هستند، پروتکل IPsec را پشتیبانی می‌کنند.

۴,۱ نحوه‌ی استفاده و ویژگی‌های اصلی امنیتی هدف ارزیابی

کلاینت VPN به کاربران راه دور اجازه می‌دهد تا از کامپیوترهای کلاینت جهت ایجاد یک تونل IPsec رمز شده برروی شبکه عمومی محافظت نشده به سمت یک شبکه خصوصی استفاده کنند (شکل ۱). هدف ارزیابی بین شبکه عمومی و موجودیت‌هایی (نرم‌افزار، کاربران و ...) که بر روی کلاینت‌های VPN تحت سیستم‌عامل مستقر شده‌اند، قرار می‌گیرد. بسته‌های IP که از شبکه خصوصی به شبکه عمومی می‌روند در صورتی رمز خواهند شد که مقصدشان کلاینت VPN دسترسی راه دور است و از خط‌مشی‌های VPN همانند شبکه مبدأ پشتیبانی می‌کنند. کلاینت VPN از داده‌ی بین خود و دروازه VPN محافظت می‌کند، حتی اگر این داده در یک شبکه عمومی به پیمایش در بیاید محرمانگی، صحت و حفاظت از داده‌ی منتقل شده حفظ می‌شود.

---

[1] Security Assurance Requrement (SAR)



شکل ۱- VPN Client

الزامات کارکرد امنیتی اصلی در این پروفایل حفاظتی، که شاخصه‌های اصلی کلاینت VPN است، عبارتند از:

- احراز هویت دروازه VPN
- محافظت رمزنگاری از داده‌های منتقل شده
- پیاده‌سازی سرویس‌ها

کلاینت VPN می‌تواند با دیگر کلاینت‌های VPN یا یک دروازه VPN یک اتصال VPN برقرار کند (که در اتصالات VPN نقطه پایانی راه دور می‌باشد). نقاط پایانی VPN یکدیگر را احراز هویت می‌کنند تا اطمینان یابند که با یک موجودیت IT خارجی مجاز در ارتباط هستند. احراز هویت دروازه VPN به عنوان بخشی از مذاکرات تبادل کلید

اینترنت (IKE) انجام می‌شود. مذاکرات IKE از زیرساخت کلید عمومی از پیش موجود برای احراز هویت استفاده می‌کند و می‌تواند به طور اختیاری از یک کلید از پیش به اشتراک گذاشته شده استفاده کند. زمانیکه IKE تکمیل شد، یک تونل IPsec امن شده با ESP [1] برقرار می‌شود.

فرض شده است که کلاینت VPN به طور مناسبی پیاده‌سازی شده است و هیچ اشتباه طراحی مهمی در آن وجود ندارد.

کلاینت VPN جهت اجرای مناسب و هم‌چنین ساز وکارهای حفاظتی ماشین کلاینتی که در ادامه مطرح شده است، به محیط IT متکی است:

- بازبینی ممیزی
- ذخیره ممیزی
- شناسایی و احراز هویت
- مدیریت امنیت
- مدیریت نشست

لازم است فروشنده راهنمای پیکربندی به مشتری ارائه دهد تا بتواند هدف ارزیابی را به صورت صحیح نصب کند و برای هر محیط عملیاتی پشتیبانی شده، ماشین کلاینت و هدف ارزیابی را سرپرستی کند.

1 Encapsulating Security Payload

۴,۲ رمزنگاری

انتظار می‌رود کلاینت VPN مبتنی بر پروتکل IPsec تمام اطلاعاتی را که بین کلاینت VPN و دروازه VPN، در جریان است رمز کند. کلاینت VPN به عنوان نقطه پایانی تونل VPN مبتنی بر پروتکل IPsec به کار می‌رود و برخی عملکردهای رمزنگاری را جهت نگهداری و برقراری تونل انجام می‌دهد. اگر جهت احراز هویت، تولید کلید و رمز کردن اطلاعاتی از رمزنگاری قوی استفاده شود و هم‌چنین پیاده‌سازی آن دارای اشتباه طراحی مهمی نباشد، حمله‌گر قادر به جستجوی فضای کلید رمزنگاری جهت به دست آوردن داده نخواهد بود. مطابق با استانداردهای پروتکل IPsec، با استفاده مناسب از یک تولید کننده بیت تصادفی[1] و فاکتورهای احراز هویت امن، اطمینان داده خواهد شد که دستیابی به اطلاعات منتقل شده با تلاشی کمتر از جستجوی کامل فضای کلید به دست نخواهد آمد. هر متن مخفی، کلیدهای خصوصی یا دیگر پارامترهای امنیتی رمزنگاری زمانی‌که دیگر استفاده نمی‌شوند صفر خواهند شد تا از افشای داده‌ی مهم امنیتی جلوگیری شود.

1 Random Bit Generator

۵ تعریف مسائل امنیتی

۵,۱ فرضیات

A.TYPE	توضیحات
A.NO_TOE_BYPASS	اطلاعات نمی‌تواند به سوی شبکه‌ای جریان یابد که میزبان VPN client بدون پذیرفته شدن از طریق هدف ارزیابی، به شبکه متصل شده باشد.
A.PHYSICAL	فرض می‌شود امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌ی آن، توسط محیط ارائه می‌شود.
A.TRUSTED_ADMIN	سرپرستان هدف ارزیابی افراد مطمئنی هستند که تمام مستندات راهنمایی را به صورت قابل اطمینانی دنبال و اعمال می‌کنند.

۵,۲ تهدیدها

T.TYPE	توضیحات
T.TSF_FAILURE	در صورت شکست خوردن سازوکارهای امنیتی هدف ارزیابی، عملکرد امنیتی هدف ارزیابی نیز به خطر می‌افتد.
T.UNAUTHORIZED_ACCESS	کاربر ممکن است به داده‌های هدف ارزیابی و کد اجرایی هدف ارزیابی، دسترسی غیرمجازی داشته باشد. کاربر مخرب،

T.TYPE	توضیحات
	پروسه، یا موجودیت IT مجاز ممکن است خود را به عنوان یک موجودیت مجاز معرفی کند تا به داده یا منابع هدف ارزیابی دستیابی غیرمجاز داشته باشد. یک کاربر مخرب، پروسه، یا موجودیت IT خارجی ممکن است خود را به عنوان هدف ارزیابی نشان دهد و داده‌های شناسایی و احراز هویت را به دست آورد.
T.UNAUTHORIZED_UPDATE	یک بخش مخرب، تلاش می‌کند تا بروزرسانی از محصول به کاربر ارائه کند که ویژگی‌های امنیتی هدف ارزیابی را به خطر اندازد.
T.USER_DATA_REUSE	داده کاربری ممکن است سهواً به مقصدی فرستاده شود که مدنظر فرستنده نبوده است.

۵,۳ خط‌مشی‌ها

T.TYPE	توضیحات
P.COMPATIBILITY	هدف ارزیابی باید برای پیاده‌سازی پروتکل‌ها از الزامات RFC تبعیت کند تا بتواند با استفاده از پروتکل‌های مشابه با دیگر تجهیزات شبکه بکار رود.
P.CONFIGURABILITY	هدف ارزیابی باید قابلیت پیکربندی ویژگی‌های مربوط به امنیت عملیاتش را ارائه دهد.

۶ اهداف امنیتی

۶,۱ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.AUTH_COMM	هدف ارزیابی امکانی ارائه خواهد داد تا اطمینان حاصل کند که کاربران با موجودیت‌هایی که وانمود می‌کنند، ارتباطی برقرار نمی‌کنند و هدف ارزیابی با موجودیت IT مجاز ارتباط برقرار می‌کند و با موجودیت‌های که به عنوان موجودیت مجاز وانمود می‌کنند، ارتباط برقرار نمی‌کنند.
O.CRYPTOGRAPHIC_FUNCTIONS	هدف ارزیابی توانایی رمزنگاری و رمزگشایی داده را ارائه خواهد کرد تا محرمانگی حفظ شود و اجازه می‌دهد تا داده‌های عملکرد امنیتی هدف ارزیابی که خارج از هدف ارزیابی منتقل می‌شوند تغییر شکل یابند (رمز شوند) و آشکار شوند (رمزگشایی شوند).
O.GW_AUTHENTICATION	هدف ارزیابی VPN gateway را که در تلاش برای برقراری یک ارتباط امن است احراز هویت خواهد کرد
O.PROTOCOLS	هدف ارزیابی اطمینان خواهد داد که پروتکل‌های استاندارد شده در هدف ارزیابی براساس RFC و/یا مشخصات صنعتی پیاده‌سازی شده است تا از قابل کاربرد بودنش اطمینان حاصل شود.

O.TYPE	توضیحات
O.RESIDUAL_INFORMATION_CLEARING	هدف ارزیابی اطمینان خواهد داد که داده موجود در منبع محافظت شده، در زمان تخصیص مجدد منبع در دسترس قرار نخواهد گرفت.
O.TOE_ADMINISTRATION	هدف ارزیابی سازوکارهایی ارائه خواهند داد تا سرپستان قادر به پیکربندی هدف ارزیابی باشند.
O.TSF_SELF_TEST	هدف ارزیابی قابلیت آزمون زیرمجموعه‌ای از عملکردهای امنیتی را ارائه خواهد داد تا از صحت عملکردش اطمینان حاصل شود.
O.VERIFIABLE_UPDATES	هدف ارزیابی قابلیتی را ارائه خواهد کرد تا اطمینان حاصل شود که بروزرسانی هدف ارزیابی توسط سرپرست تائید شده، بدون تغییر و از یک منبع قابل اطمینان است.

۶,۲ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.NO_TOE_BYPASS	اطلاعات نمی‌تواند به سوی شبکه‌ای جریان یابد که میزبان VPN client بدون پذیرفته شدن از طریق هدف ارزیابی، به شبکه متصل شده باشد.
OE.PHYSICAL	امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌های آن، توسط محیط ارائه می‌شود.

OE.TRUSTED_ADMIN	سرپرستان هدف ارزیابی جهت دنبال کردن و به کاربردن مطمئن تمام راهنماهای سرپرستی، قابل اعتماد می‌باشند.

۷ الزامات کارکرد امنیتی

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.

شماره آیتم	نام کلاس	الزام	نام الزام
۱	کلاس پیشتیبانی از رمزنگاری (FCS)	FCS_CKM.4	مدیریت کلید رمزنگاری
		FCS_COP.1	عملیات رمزنگاری
۲	کلاس حفاظت از داده‌های کاربری (FDP)	FDP_ACC.1	زیرمجموعه کنترل دسترسی
		FDP_ACF.1	مشخصه‌های امنیتی براساس کنترل دسترسی
		FDP_IFC.1	زیرمجموعه کنترل جریان اطلاعات
		FDP_IFF.1	مشخصه‌های امنیتی ساده
۳	کلاس شناسایی و احرازهویت (FIA)	FIA_PMG_EXT.1	مدیریت رمز عبور

شماره آیتم	نام کلاس	الزام	نام الزام
		FIA_AFL.1	اداره کردن شکست در احرازهویت
		FIA_ATD.1	تعریف صفات کاربری
		FIA_UAU.1	زمانبندی احرازهویت
		FIA_UAU_EXT.2	سازوکار احرازهویت براساس رمزعبور
		FIA_UID.1	شناسایی کاربر
۴	کلاس مدیریت امن (FMT)	FMT_MOF.1	مدیریت رفتار توابع امنیتی
		FMT_MTD.1	مدیریت داده‌های توابع امنیتی هدف ارزیابی
		FMT_SMF.1	مشخصات عملکردهای مدیریتی
		FMT_SMR.1	نقش‌های امنیتی
		FMT_REV.1	لغو
		FMT_MSA.1	مدیریت مشخصه‌های امنیتی

شماره آیتم	نام کلاس	الزام	نام الزام
۵	کلاس حفاظت از توابع امنیتی هدف ارزیابی (FPT)	FPT_ITT.1	محافظت از انتقال داده‌های داخل توابع امنیتی هدف ارزیابی
		FPT_STM.1	مهرهای زمانی
۶	کلاس کانال‌ها/مسیرهای مورد اعتماد (FTP)	FTP_TRP.1	مسیر مطمئن

۷,۱ کلاس پشتیبانی از رمزنگاری

در ادامه مؤلفه‌های 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 برآورده شدن چندین هدف امنیتی سطح بالا کمک کنند، از جمله اهداف امنیتی می‌توان به موارد زیر اشاره کرد:

- 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 این پیاده‌سازی می‌تواند در نرم‌افزار، سخت‌افزار و میان افزار صورت گیرد.

- **خانواده مدیریت کلید رمزنگاری[1]**

کلیدهای رمزنگاری باید از طریق دوره حیاتشان مدیریت شوند. این خانواده برای پشتیانی 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[2]**

---

1 Cryptographic key management(FCS_CKM)

2 Cryptographic operation(FCS_COP)

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 امضاء دیجیتال، تولید کنترل[1] رمزنگاری برای صحت و یا تائید کنترل، درهم‌سازی امن (خلاصه پیام)، رمزنگاری و/یا رمزگشایی کلید رمزنگاری و توافق کلید رمزنگاری می‌باشد.

شماره	نام خانواده	عنصر امنیتی
الزام		
۱	تولید کلید رمزنگاری (FCS_CKM)	**نام عنصر: مدیریت کلید رمزنگاری ۱** **شماره مؤلفه: رز-م‌ک.۱،۱ (FCS_CKM.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری نامتقارن را که برای ایجاد کلید استفاده می‌شوند مطابق الگوهای زیر تولید کنند: • استاندارد NIST SP 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته» برای طرح

1 checksum

شماره	نام خانواده

عنصر امنیتی

الزام

برقراری کلید متناهی مبتنی بر میدان[1]

- استاندارد NIST 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته[2]» برای برقراری طرح کلید مبتنی بر منحنی بیضوی[3] و پیاده‌سازی "NIST Curves" در P-256 و P-384 و [انتخاب: *P-521* ، هیچ منحنی دیگری] (چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده است)

[انتخاب:

استاندارد NIST SP 800-56 B، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری تجزیه عدد صحیح[4] برای طرح برقراری کلید مبتنی بر RSA»]

همچنین اندازه‌ی این کلید باید معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد.

---

1 Field-bsae

2 Discrete Logarithm Cryptography”

3 Curve-base

4 Integer Factorization Cryptography

شماره **نام خانواده**

عنصر امنیتی

الزام

نکته کاربردی:

این مؤلفه هدف ارزیابی را قادر می‌سازد تا برای پروتکل‌های مختلف رمزنگاری (برای مثال IPsec) که توسط هدف ارزیابی استفاده می‌شوند، جفت کلید عمومی/خصوصی تولید کنند.

از آنجا که پارامترهای دامنه مورد استفاده، توسط الزامات پروتکل در پروفایل حفاظتی مشخص شده‌اند، زمانی‌که هدف ارزیابی با پروتکل تعریف شده در این پروفایل حفاظتی مطابقت دارد، نیازی به اعتبار سنجی آنها نیست.

۲ **نام عنصر: مدیریت کلید رمزنگاری(برای کلیدهای نامتقارن-IKE) ۱ (۲)**

شماره مؤلفه: رز-م‌ک.۱,۱(۲) ((FCS_CKM.1.1(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مطابق با استاندارد [انتخاب:

- FIPS PUB 186-3، *« استاندارد امضای دیجیتال (DSS)»، پیوست b.3 برای طرح RSA*
- *FIPS PUB 186-3، «استاندارد امضای دیجیتال (DSS)، پیوست b.3 برای طرح ECDSA و پیاده‌سازی منحنی‌های NIST» -P*

شماره	نام خانواده	عنصر امنیتی
الزام		

256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر]

- *ANSI X9.31-1998، پیوست A.2.4 با استفاده از AES برای طرح RSA*]

کلیدهای رمزنگاری نامتقارن جهت استفاده در احراز هویت همتای IKE تولید کنند همچنین اندازه‌ی کلید رمزنگاری باید معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد.

نکته کاربردی:

در قسمت انتخاب این الزام، از استاندارد ANSI X9.31-1998 نیز استفاده شده است اما این استاندارد در نسخه‌های بعدی پروفایل حفاظتی حذف خواهد شد. در حال حاضر انتخاب به FIPS PUB 186-3 محدود نشده است تا به صنعت، فرصت داده شود به جای استانداردهای قبلی تولید کلید از استاندارد FIPS PUB 186-3 استفاده کند.

کلیدهایی که لازم است توسط هدف ارزیابی از طریق این الزام تولید شوند، برای احراز هویت همتای VPN در طول تبادلات کلید IKE (v1 یا v2) استفاده می‌شوند. کلید عمومی توسط مرکز صدور گواهینامه در محیط عملیاتی با یک شناسه در گواهینامه X509v3 همبسته می-شود.

شماره	نام خانواده

عنصر امنیتی

الزام

همان‌گونه که در الزام (رز-IPsec-(ت‌س).۱) نشان داده شده است، هدف ارزیابی جهت احراز هویت همتا، ملزم به پیاده‌سازی الگوریتم RSA یا ECDSA (یا هردو) می‌باشد. اندازه کلیدهایی که از کلیدهای ۲۰۴۸ بیتی RSA تولید شده است، باید معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد. همان طور که در استاندارد NIST SP 800-57، «پیشنهاداتی برای مدیریت کلید» اطلاعاتی مرتبط با قدرت کلیدِ معادل، مطرح شده است.

۳ **نام عنصر: مدیریت کلید رمزنگاری ۴**

شماره مؤلفه: رز-م‌ک-(ت‌س).۱,۴ (FCS_CKM.4.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید تمام کلیدهای رمزنگاری خصوصی و مخفی و پارامترهای مهم امنیتی[1] رمزنگاری را که دیگر مورد استفاده قرار نمی‌گیرند، صفر کند.

نکته کاربردی:

[1] Critical Security Parameter (CSP)

شماره **نام خانواده**

عنصر امنیتی

الزام

هرگونه اطلاعات مرتبط امنیتی (هم‌چون کلید، داده احراز هویت و رمز عبور) باید زمانی‌که دیگر مورد استفاده قرار نمی‌گیرد، صفر شود تا از فاش شدن و تغییر داده‌های مهم امنیتی جلوگیری شود.

هنگامی که کلید/پارامتر مهم امنیتی رمزنگاری به مکان دیگری منتقل می شود، عمل صفرسازی که در بالا اشاره شد به هر ناحیه ذخیره-سازی میانی کلید/پارامتر مهم امنیتی رمزنگاری (یعنی هر دستگاه ذخیره‌سازی مانند بافرهای حافظه که در مسیر چنین داده‌هایی قرارداده شده‌اند)، اعمال می‌شود.

۴ **نام عنصر: عملیات رمزنگاری(برای رمزنگاری/رمزگشایی داده) ۱ (۱)**

شماره مؤلفه: رز-ع‌ر.۱,۱ (۱)(۱)(FCS_COP.1.1(1))

شرح مؤلفه:

عملیات رمزنگاری (**FCS_COP**)

توابع امنیتی هدف ارزیابی باید [**رمزنگاری و رمزگشایی**] را مطابق با الگوریتم رمزنگاری AES که در مود **CBC**، **GCM**، [اختصاص: **یک یا بیش از یک مود، هیچ مود دیگر**] عمل می‌کند و اندازه‌ی کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی و [انتخاب: *۱۹۲ بیتی، نه هیچ اندازه دیگری*] مطابق با استاندارد:

- استاندارد FIPS PUB 197

شماره	نام خانواده

عنصر امنیتی

الزام

- NIST SP 800-38A، NIST SP 800-38D
- [انتخاب: *NIST SP 800-38B, NIST SP 800-38C NIST SP 800-38E* , *هیچ استاندارد دیگر*] انجام بدهند.

نکته کاربردی:

این پروفایل حفاظتی به مودهای GCM و CBC نیاز دارد تا در پروتکل‌های IPsec و IKE استفاده شود (رز-اپ-(ت‌س).۴,۱.، رز-اپ-(ت-س).۶,۱). این مؤلفه در پروفایل حفاظتی تجهیزات شبکه نیز آمده است، اما در این پروفایل حفاظتی دو مود CBC و GCM اضافه شده است تا با الزامات مربوط به پروتکل IPsec سازگار باشد و در سند هدف امنیتی نیز این دو مود در نظر گرفته شود.

۵ **نام عنصر: عملیات رمزنگاری(برای امضای دیجیتال) ۱ (۲)**

شماره مؤلفه: رز-ع‌ر.۱,۱ (۲)((FCS_COP.1.1(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید خدمات رمزنگاری امضا را مطابق با الگوریتم‌های زیر انجام بدهند:

[انتخاب:

شماره **نام خانواده**

عنصر امنیتی

الزام

- *الگوریتم امضای دیجیتال[1] با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-3، «استاندارد امضای دیجیتال»*
- *الگوریتم امضای دیجیتال RSA[2] با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-2 یا FIPS PUB 186-3، «استاندارد امضای دیجیتال»*
- *الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA[3]) با کلید ۲۵۶ بیتی یا بیشتر مطابق با*
  - *FIPS PUB 186-3، «استاندارد امضای دیجیتال»*
  - *عملکرد امنیتی هدف ارزیابی باید منحنی‌های استاندارد[4] P-256، P384 و [انتخاب: P251 ، نه سایر منحنی‌ها] (همچنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده‌است)] را پیاده‌سازی کند.]*

1 Digital Signature Algorithm (DSA)

2 RSA Digital Signature Algorithm (rDSA)

3 Elliptic Curve Digital Signature Algorithm (ECDSA)

4 NIST curves

شماره	نام خانواده

عنصر امنیتی

الزام

۶ **نام عنصر: عملیات رمزنگاری(درهم‌سازی رمزنگاری) ۱ (۳)**

شماره مؤلفه: رز-ع‌ر.۱,۱ (۳)((FCS_COP.1.1(3))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [**خدمات درهم‌سازی رمزنگاری**] را مطابق با یک الگوریتم رمزنگاری مشخص [انتخاب:*SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*] و اندازه‌ی خلاصه پیام[1][انتخاب: *۱۶۰،۲۲۴، ۲۵۶، ۳۸۴ و ۵۱۲ بیت*] که مطابق با استاندارد FIPS 180-3، «استاندارد درهم‌ساز امن» باشد، انجام دهد.

نکته کاربردی:

انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد، به طور مثال اگر الگوریتم SHA-1 انتخاب شده است، تنها انتخاب، اندازه خلاصه پیام قابل قبول ۱۶۰ بیت خواهد بود.

۷ **نام عنصر: عملیات رمزنگاری ۱(۴)**

[1] Message Digest Sizes

شماره **نام خانواده**

عنصر امنیتی

الزام

شماره مؤلفه: رز-ع‌ر.۱,۱(۴) ((FCS_COP.1.1(4))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید **[احراز هویت پیام مبتنی بر درهم‌سازی-کلید]** را مطابق با الگوریتم رمزنگاری مشخصHMAC- [انتخاب:*SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*]، با اندازه کلید [اختصاص: **اندازه کلید (بیت) استفاده شده در HMAC**]، و اندازه‌ی خلاصه پیام [انتخاب: *۱۶۰،۲۲۴، ۲۵۶، ۳۸۴ و ۵۱۲ بیت*] که مطابق با FIPS 198-1، «کد احراز هویت پیام مبتنی بر درهمسازی-کلید» و FIPS 180-3، «استاندارد درهم‌ساز امن» باشد، انجام بدهند.

نکته کاربردی:

انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد، به طور مثال اگر HMAC-SHA-256 انتخاب شده است، تنها انتخاب، اندازه خلاصه پیام قابل قبول ۲۵۶ بیت خواهد بود.

اندازه خلاصه پیام‌های بالا متناسب با الگوریتم درهم‌سازی مورد استفاده می‌باشد. کوتاه شدن خروجی HMAC پس از محاسبه درهم‌سازی گام مناسب در طیفی از برنامه‌های کاربردی است. کوتاه شدن پیام، اندازه خروجی نهایی و استانداردی که پیام کوتاه شده منطبق برآن است باید در سند هدف امنیتی بیان شود.

شماره	نام خانواده	عنصر امنیتی
الزام		
۸		**نام عنصر: پروتکلIPsec ۱** **شماره مؤلفه: رز-اپ-(تس).۱,۱ (FCS_IPSEC_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید معماری IPsec را به صورت مشخص شده در RFC 4301 پیاده‌سازی کنند.
۹	پروتکل IPsec (**FCS_IPSEC_EXT**)	**نام عنصر: پروتکلIPsec ۱** **شماره مؤلفه: رز-اپ-(تس).۱,۲ (FCS_IPSEC_EXT.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [انتخاب: *مود تونل*، *مود انتقال*] را پیاده‌سازی کنند.
۱۰		**نام عنصر: پروتکلIPsec ۱** **شماره مؤلفه: رز-اپ-(تس).۱,۳ (FCS_IPSEC_EXT.1.3)** **شرح مؤلفه:**

شماره	نام خانواده

عنصر امنیتی

الزام

توابع امنیتی هدف ارزیابی باید در انتهای لیست پایگاه داده خط‌مشی‌های امنیتی[1] به صورت دقیق، عنصری داشته باشند که هر ارتباطی که با هیچ عنصر دیگری در این پایگاه داده تطابق نداشته باشد، با آن عنصر انتهایی تطابق داشته باشد و باعث رد شدن آن ارتباط شود.

۱۱ **نام عنصر: پروتکل IPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۴,۱.(FCS_IPSEC_EXT.1.4)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید ESPدر پروتکل IPsec را به صورت تعریف شده در RFC 4303 و با استفاده از الگوریتم‌های AES-GCM-128، AES-GCM-256 که در RFC 4106 مشخص شده است، [انتخاب: *AES-CBC-128، AES-CBC-256 (هر دو در RFC 3602 مشخص شده است) همراه با الگوریتم درهم‌سازی امن مبتنی بر HMAC، هیچ الگوریتم دیگری*]پیاده‌سازی کنند.

۱۲ **نام عنصر: پروتکل IPsec ۱**

1 -Security policy database

شماره **نام خانواده**

عنصر امنیتی

الزام

شماره مؤلفه: رز-اپ-(ت‌س).۵,۱ (FCS_IPSEC_EXT.1.5)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید پروتکل

[انتخاب:

IKE1 به صورت تعریف شده در RFC های 2407، 2408، 2409، RFC 4109، [انتخاب: هیچ RFC دیگری برای اعداد متوالی توسعه یافته، RFC 4304 برای اعداد متوالی توسعه یافته] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]؛

IKE2 به صورت تعریف شده در RFC 5996 و [انتخاب: هیچ RFC دیگری برای عملیات درهم‌سازی، RFC 4868 برای عملیات درهم-سازی] را پیاده‌سازی کنند.

۱۳ **نام عنصر: پروتکل IPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۶,۱ (FCS_IPSEC_EXT.1.6)

شرح مؤلفه:

شماره	نام خانواده
	عنصر امنیتی
	الزام

توابع امنیتی هدف ارزیابی باید اطمینان بدهند که سرآیند[1] رمزنگاری شده در پروتکل [انتخاب: *IKE1، IKE2*]، از الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-256 به صورت مشخص شده در RFC 6379 و [انتخاب: *AES-GCM-128، AES-GCM-256 به صورت مشخص شده در RFC 5282، هیچ الگوریتم دیگر*] استفاده می‌کنند.

۱۴	**نام عنصر: پروتکل IPsec ۱**
	شماره مؤلفه: رز-اپ-(ت‌س).۷,۱.(FCS_IPSEC_EXT.1.7)
	شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تبادلات فاز ۱ پروتکل IKEv1 تنها از مود اصلی استفاده می‌کند.

نکته کاربردی:

تنها زمانی این الزام کاربردی است که پروتکل IKE1 انتخاب شده باشد.

1 -Payload

شماره **نام خانواده**

عنصر امنیتی

الزام

۱۵ **نام عنصر: پروتکلIPsec ۱**

شماره مؤلفه: رز-اپ-(تس).۸,۱.۸ (FCS_IPSEC_EXT.1.8)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که

[انتخاب:

- *دوره‌ی حیاتSA مربوط به IKEv2 می‌تواند توسط [انتخاب: سرپرست، دروازه VPN] براساس تعداد بسته/تعداد بایت یا بازه زمانی پیکربندی شود، به‌طوری‌که بازه زمانی محدود باشد به: ۲۴ ساعت برای فاز۱ SA و ۸ ساعت برای فاز ۲ SA،*
- *دوره‌ی حیاتSA مربوط به IKEv1 می‌تواند توسط [انتخاب: سرپرست، دروازه VPN] براساس تعداد بسته/تعداد بایت یا بازه زمانی پیکربندی شود، به‌طوری‌که بازه زمانی محدود باشد به: ۲۴ ساعت برای فاز۱ SA و ۸ ساعت برای فاز ۲* SA]

نکته کاربردی:

نویسنده هدف امنیتی باید با توجه به نسخه پروتکل IKE (IKEv1 یا IKEv2)که در پیاده‌سازی آن استفاده شده است، یکی از دو انتخاب

شماره	نام خانواده	عنصر امنیتی
الزام		

بالا را برگزیند. سپس نویسنده باید مشخص کند که چه موجودیتی مسئول پیکربندی دوره‌ی حیات SA است.

هدف ارزیابی می‌تواند دوره حیات SA را براساس تعداد بایت منتقل شده یا تعداد بسته منتقل شده محدود کند.

۱۶ **نام عنصر: پروتکل IPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۹,۱ (FCS_IPSEC_EXT.1.9)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مقدار رمز x را تولید کنند که در تبادلات کلید الگوریتم Diffie-Hellman پروتکل IKE استفاده می‌شود. این مقدار x با استفاده از عنصر تولید بیت تصادفی که در الزام (رز-ب‌ت-(ت‌س).۱) مشخص شده است، تولید می‌شود. اندازه این مقدار رمز حداقل [اختصاص: (**یک یا بیش از یک**) **عدد از بیت‌هایی که حداقل دو برابر مقدار «بیت‌های امنیتی» مربوط به گروه مذاکره Diffie-Hellman** (**که در جدول ۲ از NIST SP 800-57 لیست شده است، پیشنهادی برای مدیریت کلید- بخش ۱: کلیات**) **باشد**] بیت باشد.

۱۷ **نام عنصر: پروتکل IPsec ۱**

شماره	نام خانواده	عنصر امنیتی	الزام

شماره مؤلفه: رز-اپ-(تس).۱۰,۱ (FCS_IPSEC_EXT.1.10)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید عدد تصادفی(nonce) را تولید کنند که در تبادلات IKE استفاده می‌شود به طوری که احتمال تکرار این عدد در دوره حیات SA مربوط به پروتکل IPsec کمتر از ۱ در ۲^۸ [اختصاص: **(یک یا بیش از یک) مقدار «بیت‌های امنیتی» مربوط به گروه مذاکره Diffie-Hellman (که در جدول ۲ از NIST SP 800-57 لیست شده است، پیشنهادی برای مدیریت کلید- بخش ۱: کلیات) باشد**] است.

۱۸ **نام عنصر: پروتکل IPsec ۱**

شماره مؤلفه: رز-اپ-(تس).۱۱,۱ (FCS_IPSEC_EXT.1.11)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE گروه‌های Diffie-Hellman ۱۴(2048-bit MODP)، ۱۹ (256-bit MODP) و [انتخاب: *۵ (1536-bit MODP)، ۲۴ (2048-bit MODP با 256-bit POS)*، ۲۰ *(384-bit Random ECP)*، *[اختصاص:*

شماره **نام خانواده**

عنصر امنیتی

الزام

دیگر گروه‌های DH که توسط هدف ارزیابی پیاده‌سازی شده‌اند]، *هیچ گروه DH دیگر*] را پیاده‌سازی می‌کنند.

نکته کاربردی:

در این الزام با استفاده از بخش انتخاب، می‌توان گروه‌های Diffie-Hellman بیشتری پشتیبانی کرد. هم‌چنین این الزام برای تبادلات IKEv1 و IKEv2 استفاده می‌شود. در نسخه‌های بعدی این پروفایل حفاظتی، DH گروه ۲۰ (384 بیت RandomECP) لازم است. باید توجه شود در صورت اضافه کردن گروه DH، باید با الزامات لیست شده در الزام (رز-م‌ک.۱) مطابقت داشته باشد.

۱۹ **نام عنصر: پروتکل IPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۱۲,۱ (FCS_IPSEC_EXT.1.12)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE با استفاده از الگوریتم [انتخاب: *RSA*، *ECDSA*] احراز هویت همتا را انجام می‌دهند و از گواهینامه‌ی X.509v3 مطابق با RFC 4945 و [انتخاب: *کلیدهای از پیش به اشتراک گذاشته شده*، *هیچ روش دیگری*]، جهت احراز هویت استفاده می‌کنند.

شماره **نام خانواده**

عنصر امنیتی

الزام

نکته کاربردی:

برای اهداف ارزیابی مطابق با این پروفایل حفاظتی، حداقل یک روش احراز هویت مبتنی بر کلید عمومی لازم و ضروری است. نویسنده هدف امنیتی یک یا بیش از یک طرح کلید عمومی را که توسط هدف ارزیابی پیاده‌سازی شده است انتخاب می‌کند. در بخش خلاصه مشخصات هدف ارزیابی، به طور دقیق روشی که این الگوریتم‌ها استفاده می‌کند شرح داده شده است (برای مثال، RFC2409 با استفاده از کلید عمومی، سه روش احرازهویت معرفی می‌کند، هر یک از این روش‌ها که پشتیبانی شود در بخش خلاصه مشخصات هدف ارزیابی در سند هدف امنیتی شرح داده می‌شود).

۲۰ **نام عنصر: پروتکلIPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۱۳,۱ (FCS_IPSEC_EXT.1.13)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید بتوانند به صورت پیش‌فرض اطمینان دهند که الگوریتم متقارن پیشنهاد شده جهت حفاظت اتصال [انتخاب: *فاز ۱ IKEv1، IKEv2 SA IKE*] از نظر قدرت، بزرگتر یا معادل الگوریتم متقارن (تعداد بیت‌های کلید) پیشنهاد شده جهت حفاظت اتصال

شماره **نام خانواده**

عنصر امنیتی

الزام

[انتخاب: *فاز ۲ IKEv1، IKEv2 CHILD_SA*] هستند.

نکته کاربردی:

نویسنده‌ی هدف ارزیابی با توجه به پروتکلی که در هدف ارزیابی پیاده‌سازی شده است، یک یا هر دو پروتکل IKE را انتخاب می‌کند. بدیهی است که نسخه IKE انتخاب شده نه تنها باید در این مؤلفه سازگار باشد، بلکه باید با دیگر مؤلفه‌های این عنصر نیز سازگار باشد.

۲۱ **نام عنصر: تولید بیت تصادفی ۱**

شماره مؤلفه: رز-ب‌ت.۱،۱ (FCS_RBG.1.1)

شرح مؤلفه:

تولید بیت تصادفی

(FCS_RBG_EXT)

توابع امنیتی هدف ارزیابی باید تمام خدمات تولید بیت تصادفی را مطابق با [انتخاب: یکی از: *استاندارد NIST 800-90 با استفاده از الگوریتم [انتخاب: Hash_DRBG (هرکدام)، HMAC_DRBG(هرکدام)، Dual_EC_DRBG.CTR_DRBG (AES) (هرکدام)]، پیوست C استاندارد FIPS Pub 140-2، ضمیمه ۲،۴ از استاندارد X9.31 با استفاده از الگوریتم AES*] انجام بدهند که توسط یک منبع آنتروپی ورودی اولیه داده می‌شوند، آنتروپی از [انتخاب: یکی یا هر دو : *منبع نویز مبتنی بر نرم‌افزار توابع امنیتی هدف ارزیابی، نویز مبتنی بر سخت‌افزار توابع*

شماره **نام خانواده**

عنصر امنیتی

الزام

امنیتی هدف ارزیابی] محاسبه می‌شود.

نکته کاربردی:

در اولین انتخاب این الزام، نویسنده هدف امنیتی باید استانداردی را که مطابق با خدمات RBG است، انتخاب کند.(یا NIST 800-90 یا پیوست C استاندارد FIPS.)

استاندارد SP 800-90 در برگیرنده‌ی چهار روش متفاوت برای تولید اعداد تصادفی می‌باشد که هرکدام از این روش‌ها به اصول اولیه رمزنگاری (توابع درهم‌ساز/رمز) بستگی دارند. نویسنده هدف امنیتی تابع مورد استفاده برای تولید عدد تصادفی را در این الزام انتخاب خواهد کرد(اگر 800-90 انتخاب شده‌باشد) همچنین اصول اولیه رمزنگاری استفاده شده را با اضافه کردن الزام یا در بخش خلاصه امنیتی هدف ارزیابی لحاظ می‌کند.

درحالی‌که هر کدام از توابع درهم‌ساز تعریف‌شده(SHA-1, SHA-224,SHA-256, SHA-384, SHA-512) برای Hash_DRBG یا HMAC_DRBG مجاز هستند، برای CT_DRBG تنها پیاده‌سازی‌های مبتنی بر AES مجازند.

برای Dual_EC_DRBG هریک از منحنی‌های تعریف شده در استاندارد SP 800-90 مجاز هستند، نویسنده هدف امنیتی باید در سند هدف

شماره	نام خانواده	عنصر امنیتی
		الزام
		امنیتی منحنی و الگوریتم درهم‌ساز استفاده شده را لحاظ کند.
		در دومین انتخاب این الزام، نویسنده هدف امنیتی مشخص می‌کند که منبع آنتروپی مبتنی بر نرم‌افزار است یا سخت‌افزار یا هردو.
		اگر چند منبع آنتروپی وجود داشته باشد، نویسنده هدف امنیتی باید به طور دقیق منبع هر آنتروپی را مشخص کند که مبتنی بر سخت‌افزاراست یا نرم‌افزار. به طور کلی اولویت با منابع نویز مبتنی بر سخت‌افزار است.
		توجه داشته باشید که در پیوست C استاندارد FIPS 140-2، در حال حاضر تنها روش شرح داده شده در توصیه‌ی NIST، تولید کننده عدد تصادفی مبتنی بر پیوست الف.۲,۴ از ANSI X9.31 با استفاده از سه کلید سه‌تایی الگوریتم‌های DES و AES [1] در بخش ۳، معتبر می‌باشند.
		در صورتی‌که طول کلید استفاده شده در پیاده‌سازی AES با طول کلید استفاده شده در رمزنگاری داده متفاوت باشد، آنگاه باید الزام (رز-ع-ر.۱) را برای منعکس کردن طول کلید متفاوت، دو بار تکرار کرد.
۲۲		**نام عنصر: تولید بیت تصادفی ۱**

1 ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms

شماره نام خانواده

عنصر امنیتی

الزام

شماره مؤلفه: رز-ب‌ت.۲,۱ (FCS_RBG.1.2)

شرح مؤلفه:

مقدار **اولیه فرستاده شده به تابع** تولید بیت تصادفی قطعی باید حداقل [انتخاب: *۱۲۸، ۲۵۶ بیت*] آنتروپی باشد که این مقدار دست‌کم با بزرگترین طول بیت کلیدها و پارامترهای احراز هویتی که این تابع تولید خواهد کرد، برابر است.

نکته کاربردی:

در این الزام، نویسنده هدف امنیتی حداقل تعداد بیت‌های آنتروپی را که برای مقدار اولیه داده به تابع تولید بیت تصادفی استفاده شده است، انتخاب می‌کند.

۷,۲ کلاس حفاظت از داده‌های کاربری

نام کلاس: حفاظت از داده کاربری

شرح کلاس: این کلاس شامل خانواده‌هایی است که الزامات مربوط به محافظت از داده کاربر را مشخص می‌کنند. خانواده‌های محافظت از داده کاربر در چهار گروه زیر

دسته بندی شده‌اند که علاوه بر مشخصه‌های امنیتی مربوط به داده کاربری، داده‌های کاربری در داخل هدف ارزیابی را در طول ورود، خروج و ذخیره سازی نیز نشان می-دهند.

خانواده‌های این کلاس در چهار گروه زیر دسته بندی شده‌اند:

۱) خط‌مشی‌های امنیتی مربوط به محافظت از داده کاربری

- خط‌مشی‌های کنترل دسترسی (حف-س‌ک)[1]
- خط‌مشی‌های مرتبط با کنترل جریان اطلاعات (حف-خج)[2]

در این دو خانواده، به نویسنده هدف امنیتی/پروفایل حفاظتی اجازه داده می‌شود تا خط‌مشی‌های امنیتی را که برای حفاظت از داده‌کاربری در نظر گرفته شده است و همچنین حوزه کنترلی این خط‌مشی‌ها نام ببرد.

خط‌مشی‌های امنیتی نام برده شده در این دو خانواده

- خط‌مشی‌های امنیتی در نظر گرفته شده برای کنترل دسترسی

1 Access control policy(FDP_ACC)

2 Information flow control policy(FDP_IFC)

- خط‌مشی‌های امنیتی در نظر گرفته شده برای کنترل جریان اطلاعات

توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش«انتخاب» یا «اختصاص» فراخوانی می‌شوند.

در دو خانواده‌ی توابع کنترل دسترسی (حف-ت‌ک)[1] و توابع کنترل جریان اطلاعات (حف-ک‌ج)[2] قوانینی که تعریف کننده « خط‌مشی‌های امنیتی کنترل دسترسی» و « خط‌مشی‌های امنیتی کنترل جریان اطلاعات» هستند، آورده شده است.

۲) فرم‌های مختلف محافظت از داده کاربری

- توابع کنترل دسترسی (حف-ت‌ک)
- توابع کنترل جریان اطلاعات (حف-ک‌ج)
- انتقال داخلی در هدف ارزیابی (حف-اد)[3]
- حفاظت از اطلاعات باقیمانده (حف-اب)[4]

---

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)

- عملیات عقب‌گرد به منظور بازگرداندن حالت/حالت‌های قبل (حف-ع‌گ)[1]
- یکپارچگی داده‌های ذخیره شده (حف-ی‌د)[2]

۳) ورود و خروج، ذخیره‌سازی برون‌خطی[3]

- احراز هویت[4] داده (حف-ت‌د)
- صادر شده از هدف ارزیابی (حف-ص‌ا)[5]
- ورود داده‌ها از بیرون به هدف ارزیابی (حف-وب)[6]

مؤلفه‌های این خانواده، انتقال قابل اعتماد به داخل یا خارج از هدف ارزیابی را نشان می‌دهند.

۴) ارتباطات میان توابع امنیتی هدف ارزیابی

- محافظت از انتقال محرمانگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-م‌د)[1]

---

1 Rollback(FDP_ROL)

2 Stored data integrity(FDP_SDI)

3 Offline

4 Data authentication(FDP_DAU)

5 Export from the TOE(FDP_ETC)

6 Import from outside of the TOE(FDP_ITC)

- محافظت از انتقال یکپارچگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-ی‌ا)[۲]

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

- **خانواده خط‌مشی‌های کنترل دسترسی**

این خانواده خط‌مشی‌های امنیتی مربوط به کنترل دسترسی را نام می‌برد و حوزه کنترلی سیاست‌گذاری‌ها را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال[۳] تحت کنترل سیاست‌گذاری‌ها
- موجودیت‌های غیرفعال[۴] تحت کنترل سیاست‌گذاری‌ها
- عملیات بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده که توسط خط‌مشی‌های امنیتی پوشش داده می‌شود.

بنابراین در مؤلفه‌های این خانواده، خط‌مشی امنیتی نام‌برده می‌شود و برای هریک از خط‌مشی‌های امنیتی نام‌برده شده، موجودیت فعال و غیرفعال تحت کنترل آن خط-

---

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

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

3 Subject

4 Object

مشی و عملیات بین موجودیت فعال و غیرفعال نیز نام‌برده می‌شود.

در این خانواده می‌توان خط‌مشی‌های امنیتی مختلفی برای کنترل دسترسی داشت و هریک نام منحصر به فرد خود را داشته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از خط‌مشی‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-س‌ک.۱٫۱(۱)، حف-س‌ک.۱٫۱(۲)).

قوانینی که عملکرد خط‌مشی‌های امنیتی را برای کنترل دسترسی تعریف می‌کنند، در خانواده‌های توابع کنترل دسترسی (حف-ت‌ک) و صادر شده از هدف ارزیابی (حف-ص‌ا) تعریف می‌شوند.

خط‌مشی‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش«انتخاب» یا «اختصاص» فراخوانی می‌شوند.

- **خانواده توابع کنترل دسترسی**

در خانواده خط‌مشی‌های امنیتی کنترلی دسترسی (حف-س‌ک)، تنها این خط‌مشی‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای خط‌مشی امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (حف-س‌ک)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام‌برده می‌شوند.

- **خانواده احراز هویت داده**

احراز هویت داده به هر نهادی، اجازه پذیرش مسوولیت احراز صحت اطلاعات را می‌دهد (با دیجیتالی امضاء کردن اطلاعات). این خانواده روشی را مشروط بر تضمین اعتبار

یک بخش خاص از داده ارائه می‌کند که می‌تواند به منظور بررسی محتوای اطلاعات از لحاظ جعل نشدن یا تغییر یافتن مکرر مورد استفاده قرار گیرد.

- **خانواده صادرشده از هدف ارزیابی**

در دو خانواده (حف-س‌ک) و (حف-خج) خط‌مشی‌های امنیتی بر روی کنترل دسترسی و جریان اطلاعات نام‌برده شده‌اند. در این خانواده این خط‌مشی‌های امنیتی بر روی داده تحت کنترل این خط‌مشی‌ها هنگام خروج از هدف ارزیابی اعمال می‌شود، مشخصه‌های امنیتی داده‌ها هنگام صدور می‌تواند حفظ یا نادیده گرفته شود. در واقع در این خانواده محدودیت‌هایی برای صدور داده از هدف ارزیابی اعمال می‌شود.

- **خط‌مشی‌های کنترل جریان اطلاعات**

این خانواده سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات را نام می‌برد 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.

بنابراین در مؤلفه‌های این خانواده، خط‌مشی‌های امنیتی نام‌برده می‌شوند و برای هریک از خط‌مشی‌های امنیتی نام‌برده شده، موجودیت فعال و غیرفعال تحت کنترل آن

خط‌مشی و عملیات بین موجودیت فعال و غیرفعال نیز نام‌برده می‌شوند.

در این خانواده می‌توان خط‌مشی‌های امنیتی مختلفی برای کنترل دسترسی داشت و هریک نام منحصر به فرد خود را داشته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از خط‌مشی‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-خج.۱٫۱(۱)، حف-خج.۱٫۱(۲)).

قوانینی که عملکرد خط‌مشی‌های امنیتی را برای کنترل دسترسی تعریف می‌کنند، در خانواده‌های توابع کنترل دسترسی (حف-کج) و صادر شده از هدف ارزیابی (حف-ص‌ا) تعریف می‌شوند.

خط‌مشی‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش«انتخاب» یا «اختصاص» فراخوانی می‌شوند.

- **خانواده توابع کنترل جریان اطلاعات**

در خانواده خط‌مشی‌های امنیتی کنترلی دسترسی (حف-خج)، تنها این خط‌مشی‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای خط‌مشی امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (حف-خج)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل خط-مشی‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام‌برده می‌شوند.این خانواده شامل دو الزام است:

- یکی 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 باقی سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات در تعامد است. با توجه به طبیعتشان سرپیچی کردن آنها از سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات، منجر به نقص در خط‌مشی می‌شود. بنابراین، باید عملیات خاصی برای جلوگیری یا محدود کردن جریان اطلاعات غیرمجاز در نظر گرفت.

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

این خانواده تعریف کننده سازوکارهایی برای ورود داده‌های کاربری تحت کنترل خط‌مشی‌های امنیتی (خط‌مشی‌های امنیتی کنترل جریان و کنترل دسترسی) از خارج هدف ارزیابی می‌باشد. برای ورود داده باید خط‌مشی‌های تعریف شده بر روی داده اعمال شود، هم‌چنین مشخصه های امنیتی مطلوبی برای اینگونه از داده‌ها در نظر گرفته می‌شود. در واقع این خانواده محدودیت‌هایی بر روی داده‌های ورودی از خارج هدف ارزیابی اعمال می‌کند.

- **خانواده انتقال هدف ارزیابی داخلی**

این خانواده الزاماتی را ارائه می‌دهد تا از داده کاربری در زمانی‌که بین بخش‌های مجزای هدف ارزیابی در سراسر کانال داخلی[1] انتقال می‌یابد، حفاظت کند. هم‌چنین در این خانواده داده‌ها را براساس مشخصه‌های امنیتی از یکدیگر مجزا می‌کنند و برای شناسایی خطا در صحت داده، داده‌های منتقل شده بین بخش‌های هدف ارزیابی پایش می-

[1] Internal channel

شوند.

- **خانواده حفاظت از اطلاعات باقیمانده**

این خانواده اطمینان می‌دهد در زمانی‌که منبع از یک موجودیت غیرفعال آزاد می‌شود و دوباره به یک موجودیت غیرفعال دیگر اختصاص داده می‌شود، هرگونه داده موجود در منابع، در دسترس قرار نمی‌گیرد. این خانواده نیاز دارد که از هرگونه داده موجود در منابع که به طور منطقی حذف یا آزاد می‌شود، محافظت کند، اما ممکن است هنوز در داخل منابع کنترل شده توابع امنیتی هدف ارزیابی اطلاعاتی وجود داشته باشد که به موجودیت غیرفعال دیگری اختصاص داده شود.

- **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 کننده‌ی قابلیت بی‌اثر کردن عملیات یا مجموعه‌ای از عملیات است تا یکپارچگی داده کاربری را حفظ کند.

- **خانواده صحت داده‌های ذخیره شده**

این خانواده الزاماتی را ارائه می‌کند که از داده کاربری ذخیره شده در کانتینر تحت کنترل توابع امنیتی هدف ارزیابی، محافظت می‌کند. خطای صحت ممکن است داده کاربری ذخیره شده در حافظه یا در یک ابزار ذخیره‌سازی را تحت تأثیر قرار بدهند. این خانواده صحت داده‌های ذخیره شده را حفظ می‌کند و ممکن است در صورت تشخیص خطا، اقدامی در برابر آن انجام بدهد، اما خانواده «انتقال هدف ارزیابی داخلی (حف-اد)» صحت داده کاربری در حال انتقال در هدف ارزیابی را 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 صحیح داده کاربر در داخلی عملکرد امنیتی هدف ارزیابی**

این خانواده الزاماتی را تعریف می‌کند تا صحت داده کاربری را که بین هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شود، تأمین کند و داده کاربری را از خطاهای قابل تشخیص بازیابی کند. این خانواده حداقل داده کاربری را جهت اطمینان از تغییر نیافتن پایش می‌کند. همچنین، این خانواده از روش‌های مختلف جهت اصلاح خطاهای تشخیص داده شده در صحت داده پشتیبانی می‌کند.

شماره	نام خانواده	عنصر امنیتی
الزام		
۲۳		**نام عنصر: حفاظت کامل از داده های باقی مانده ۲**
حفاظت از داده های باقی مانده (FDP_RIP)		**شماره مؤلفه: ح‌ف-اب.۱,۲(FDP_RIP.2.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تضمین کنند که هرگونه محتوی اطلاعات قبلی یک منبع را در زمان [انتخاب: *تخصیص منابع به*، *آزادسازی منابع از*] تمام موجودیت های غیرفعال، غیرقابل دسترس کنند.

۷,۳ کلاس شناسایی و احراز هویت

نام کلاس: شناسایی و احراز هویت

شرح کلاس: خانواده‌های این کلاس الزاماتی برای تصدیق و تائید هویت کاربر ادعا شده تعریف کرده‌اند. برای اطمینان یافتن از آنکه کاربران همراه با مشخصه‌های امنیتی به طور مثال، هویت گروه‌ها، نقش‌ها) مناسبی می‌باشند، شناسایی و احرازهویت کاربران لازم و ضروری است.

شناسایی صریح کاربران مجاز و اختصاص صحیح مشخصه‌های 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 می آورند تا هویت کاربران تعیین و احراز هویت شوند، صلاحیت آنهایی را که با هدف ارزیابی در تعامل هستند تعیین کنند و برای هر کاربر مجاز مشخصه‌های امنیتی به طور صحیح اختصاص داده شود. موثر اجرا شدن الزامات کلاس‌های دیگر (به طور 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 شده‌اند.

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

این خانواده حاوی الزاماتی است که تعریف کننده مقادیری برای تعداد تلاش‌های ناموفق صورت گرفته جهت احراز هویت می‌باشد، هم‌چنین اقداماتی را که توابع امنیتی هدف ارزیابی در مواردی که تلاش جهت احراز هویت با شکست مواجه می‌شود، تعریف می‌کند. 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 مشخصه‌های امنیتی، به غیر از هویت کاربر که در اجرای الزامات عملکرد امنیتی استفاده شده است، باشند. این خانواده الزاماتی برای مرتبط کردن مشخصه‌های امنیتی کاربر به کاربران تعریف می‌کند تا در صورت لزوم توابع امنیتی هدف ارزیابی را در تصمیم‌گیری‌های امنیتی پشتیبانی کند.

---

1 Authentication failures(FIA_AFL)

2 User attribute definition(FIA_ATD)

- **خانواده مشخصات رازها**[1]

این خانواده تعریف کننده الزاماتی برای سازوکارهایی است که معیارهای کیفی تعریف شده را بر روی رازها اجرا می‌کنند. الزامات بر روی ساختار کلمه عبور نمونه‌ای از آن است.

- **خانواده احراز هویت کاربر**[2]

این خانواده تعریف کننده انواع سازوکارهای‌های احراز هویت کاربر و الزامات مرتبط با آن است که توسط توابع امنیتی هدف ارزیابی پشتیبانی می‌شود.

- **خانواده شناسایی کاربر**[3]

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 هستند.

- **خانواده اتصال موجودیت فعال- کاربر**[4]

یک کاربر احراز هویت شده، به منظور استفاده از توابع امنیتی هدف ارزیابی معمولاً به عنوان یک موجودیت فعال در سیستم عمل می‌کند. مشخصه‌های 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

1 Specification of secrets(FIA_SOS)

2 User authentication(FIA_UAU)

3 User identification(FIA_UID)

4 User-subject binding(FIA_USB)

را فراهم آورد.

شماره	نام خانواده	عنصر امنیتی
الزام		
۲۴		**نام عنصر: گواهینامه‌های X509. ۱**
		شماره مؤلفه: اش-X509 (ت‌س).۱,۱(FIA-X509-EXT.1.1)
	خانواده گواهینامه-های X509 (**FIA-X509**)	**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از گواهینامه‌های x509v3 به صورت تعریف شده در RFC 5280 استفاده کنند تا از احراز هویت برای IPsec و اتصالات [انتخاب: *بدون پروتکل دیگر*، *TLS*، *SSH*] پشتیبانی کنند.
		نکته کاربردی: RFC 5280 الزامات اعتبارسنجی گواهینامه و اعتبارسنجی مسیر گواهینامه را تعریف کرده است که توسط هدف ارزیابی پیاده‌سازی می‌شود.

شماره **نام خانواده**

عنصر امنیتی

الزام

۲۵ **نام عنصر: گواهینامه‌های X509.۱**

شماره مؤلفه: اش-X509 (ت‌س).۱,۳(FIA-X509-EXT.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیتی را برای سرپرستان احراز هویت شده، ارائه دهند تا گواهینامه‌های x.509v3 جهت استفاده توسط توابع امنیتی مشخص شده در این پروفایل حفاظتی، در داخل هدف ارزیابی بارگذاری شوند.

۲۶ **نام عنصر: گواهینامه‌های X509. ۱**

شماره مؤلفه: اش-X509 (ت‌س).۱,۴(FIA-X509-EXT.1.4)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید پیغام درخواست گواهینامه را به صورت مشخص شده در RFC2986 تولید کنند و بتوانند اطلاعات زیر را در این درخواست اعلام کنند: کلید عمومی، نام عمومی، سازمان، واحد سازمانی و کشور

نکته کاربردی:

شماره	نام خانواده

عنصر امنیتی

الزام

کلید عمومی اشاره شده در مؤلفه «اش-.X509۴,۱» بخش کلید عمومی از جفت کلید خصوصی- عمومی تولید شده توسط هدف ارزیابی مشخص شده در «رز-م‌ک.۱(۲)» می‌باشد.

۲۷ **نام عنصر: گواهینامه‌های X509. ۱**

شماره مؤلفه: اش-X509 (ت‌س).۸,۱(FIA-X509-EXT.1.8)

شرح مؤلفه:

اگر گواهینامه یا مسیر گواهینامه نامعتبر باشد توابع امنیتی هدف ارزیابی نباید SA[1] را برقرار کنند.

۲۸ **نام عنصر: گواهینامه‌های X509. ۱**

شماره مؤلفه: اش-X509 (ت‌س).۹,۱(FIA-X509-EXT.1.9)

شرح مؤلفه:

1 Security Association

شماره	نام خانواده

عنصر امنیتی

الزام

اگر نام مشخص[1] که در گواهینامه قرار گرفته است با نام مشخص مورد انتظار برای موجودیت‌هایی که در تلاش برای ایجاد اتصالی هستند، منطبق نباشد توابع امنیتی هدف ارزیابی نباید SA را برقرار کنند.

۲۹ **نام عنصر: گواهینامه‌های X509. ۱**

شماره مؤلفه: اش-X509 (ت‌س).۱۰,۱(FIA-X509-EXT.1.10)

شرح مؤلفه:

زمانی‌که توابع امنیتی هدف ارزیابی نمی‌توانند اتصالی را برقرار کنند تا اعتبار گواهینامه را تعیین کنند، توابع امنیتی هدف ارزیابی باید به عنوان یک انتخاب برای سرپرست، SA را برقرار کنند یا برقراری SA را نپذیرند.

نکته کاربردی:

منظور از «اش-X509-(ت‌س).۱۰,۱» آن است که چنان‌چه هدف ارزیابی نتواند به موجودیت مسئول ارائه‌ی اطلاعات اعتبارسنجی

1 Distinguished Name

شماره	نام خانواده
عنصر امنیتی	
الزام	

گواهینامه متصل شود، می‌تواند جهت اجازه برقراری نشست و یا عدم اجازه برقراری نشست تنظیم شود. برای مثال، اگر ارتباطی با CRL به علت خاموش بودن ماشین یا قطع بودن مسیر شبکه برقرار نشود، سرپرست می‌تواند هدف ارزیابی را به گونه‌ای تنظیم کند که اجازه برقراری نشست را بدهد به جای آنکه از توانایی‌های هدف ارزیابی در ایجاد یک SA به علت در دسترس نبودن CA جلوگیری کند.

۷,۴ کلاس مدیریت امنیت

در ادامه مؤلفه‌های 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. در این کلاس مشخصه‌های امنیتی، توابع و داده‌های توابع امنیتی هدف ارزیابی، نقش‌های مدیریتی مختلف و تعاملاتشان، هم‌چون جداسازی قابلیت‌ها، می‌توانند مشخص شوند.

این کلاس دارای چندین هدف است:

- مدیریت داده توابع امنیتی هدف ارزیابی برای مثال علامت‌ها[1]
- مدیریت مشخصه‌های امنیتی، برای مثال لیست‌های کنترل دسترسی و لیست قابلیت‌ها
- مدیریت کارکرد 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

خانواده های آن در ادامه آمده است.

➢ خانواده مدیریت کارکرد توابع امنیتی هدف ارزیابی[2]

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

➢ خانواده مدیریت مشخصه‌های امنیتی[3]

این خانواده اجازه کنترل کاربران مجاز را در حین مدیریت مجوزهای امنیتی می‌دهد. این مدیریت می‌تواند شامل قابلیتی برای مشاهده و تغییر مجوزهای امنیتی باشد.

---

1 Banner

2 Management of functions in TSF (FMT_MOF)

3 Management of security attributes (FMT_MSA)

- **خانواده مدیریت داده‌های توابع امنیتی هدف ارزیابی[1]**

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

- **خانواده لغو[2]**

این خانواده لغو مشخصه‌های امنیتی انواع موجودیت‌ها در هدف ارزیابی را نشان می‌دهد.

- **خانواده انقضای مشخصه امنیتی[3]**

این خانواده قادر به اعمال محدودیت زمانی برای اعتبار مشخصه‌های امنیتی می‌باشد.

- **خانواده مشخصات کارکردهای مدیریت[4]**

این خانواده اجازه می‌دهد تا مشخصات عملکردهای مدیریتی توسط هدف ارزیابی ایجاد شوند. عملکردهای مدیریتی با استفاده از ایجاد رابط توابع امنیتی هدف ارزیابی به

---

1 Management of TSF data (FMT_MTD)

2 Revocation (FMT_REV)

3 Security attribute expiration (FMT_SAE)

4 Specification of Management Functions (FMT_SMF)

سرپرستان اجازه می دهند تا پارامترهایی برای کنترل عملکرد ویژگی‌های مربوط به امنیت هدف ارزیابی تعریف کند، 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.

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

- **خانواده نقش‌های امنیتی[1]**

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	نام خانواده	عنصر امنیتی	الزام
۳۰	مشخصات کارکردهای مدیریت	**نام عنصر:** مشخصات کارکردهای مدیریت ۱ **شماره مؤلفه: م‌د-ع‌م.۱,۱ (FMT_SMF.1.1)**	

1 Security management roles (FMT_SMR)

شماره	نام خانواده	عنصر امنیتی
الزام		

(FMT_SMF) شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به انجام کارکردهای مدیریت زیر باشند:

- مشخص کردن ارتباطات امنیتی که در طول مذاکرات IKE باید باید پیشنهاد و پذیرفته شود.
- توانایی پیکربندی نسخه پروتکل IKE
- توانایی پیکربندی تکنیک‌های احراز هویت IKE
- توانایی پیکربندی زمان ارسال یا دریافت رمز برای کلیدهای نشستی که ایجاد شده‌اند. واحد اندازه‌گیری برای پیکربندی زمان ارسال و یا دریافت رمز باید بیش از یک ساعت نباشد.
- توانایی پیکربندی بررسی ابطال گواهینامه
- توانایی مشخص کردن مجموعه الگوریتم‌هایی که ممکن است در طول تبادلات IPsec پیشنهاد و پذیرفته شود.
- توانایی مشخص کردن روش‌های احراز هویت نظیر به نظیر، در صورت اجازه.
- توانایی به‌روزرسانی هدف ارزیابی، و بررسی به‌روزرسانی‌ها

شماره **نام خانواده**

عنصر امنیتی

الزام

- توانایی پیکربندی تمام کارکردهای مدیریت امنیتی که در دیگر بخش‌های این پروفایل حفاظتی معرفی شده است.
- [اختصاص: هر کارکرد مدیریتی دیگر]

نکته کاربردی:

برای نصب، کلاینت VPN جهت احراز هویت سرپرست برای ورود به ماشین کلاینت، به محیط IT متکی می‌باشد. برای پیکربندی عملکرد زمان ارسال یا دریافت رمز برای کلیدهای نشست ایجاد شده، واحد اندازه گیری باید بیش از یک ساعت نباشد. برای مثال، واحد اندازه گیری در ثانیه، دقیقه، ساعت قابل پذیرش است و واحد اندازه‌گیری بر اساس روز یا بیش از آن قابل پذیرش نیست.

در برخی موارد ممکن است دروازه VPN اطلاعات پیکربندی را به کلاینت VPN تحمیل کند. این عمل توسط سرپرست قابل قبول است، نویسنده هدف امنیتی باید به طور واضح بیان کند که کدام عملکرد مدیریتی بر روی پلتفرم مستقر بر کلاینت VPN انجام و چگونه توسط دروازه VPN انجام می‌شود.

۷٫۵ کلاس حفاظت از توابع امنیتی هدف ارزیابی

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 می‌شوند و برای صحت و یکپارچگی داده توابع امنیتی هدف ارزیابی مورد استفاده قرار می‌گیرند. از بعضی جهات ممکن است به نظر بیاید خانواده‌های این کلاس تکرار عناصر کلاس محافظت از داده کاربری است، حتی ممکن است هر دوی این کلاس‌ها با سازوکار مشابهی پیاده‌سازی شده‌باشند. 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 کنند 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، که پایگاه داده‌های سرپرستی، راهنمایی کننده‌ی اجرای عملکرد امنیتی می‌باشند.

---

1 Bypass

- موجودیت‌های خارجی که توابع امنیتی هدف ارزیابی، ممکن است جهت اجرای الزامات عملکرد امنیتی با آنها در تعامل باشند.

- **خانواده شکست امن**[1]

الزامات این خانواده اطمینان می‌دهد که هدف ارزیابی در هنگامی که مجموعه‌ای از شکست‌های مشخص در توابع امنیتی هدف ارزیابی روی می‌دهد، کارکرد امنیتی لازم اجرا می‌شود.

- **خانواده دسترس‌پذیری داده ارسال شده توابع امنیتی هدف ارزیابی**[2]

این خانواده قوانینی را تعریف می‌کند که در هنگام انتقال داده توابع امنیتی هدف ارزیابی بین توابع امنیتی هدف ارزیابی و دیگر محصولات IT از نبود دسترسی به این داده‌ها، جلوگیری می‌کند. 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 محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی**[3]

این خانواده تعریف کننده‌ی قوانینی برای محافظت از افشای غیرمجاز داده توابع امنیتی هدف ارزیابی در طول انتقال بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن

---

1 Fail secure(FPT_FLS)

2 Availability of exported TSF data(FPT_ITA)

3 Confidentiality of exported TSF data (FPT_ITC)

IT است. 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[1]**

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[2]**

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 می‌کند.

- **خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[3]**

---

1 Integrity of exported TSF data (FPT_ITI)

2 Internal TOE TSF data transfer (FPT_ITT)

3 TSF physical protection (FPT_PHP)

مؤلفه‌های حفاظت فیزیکی توابع امنیتی هدف ارزیابی به محدودیت‌هایی بر روی دستیابی فیزیکی غیرمجاز به توابع امنیتی هدف ارزیابی، بازدارندگی از اصلاح فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی و مقاومت در برابر اصلاح فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی اشاره دارند.

الزامات مؤلفه‌ها در این خانواده این اطمینان را می‌دهند که از توابع امنیتی هدف ارزیابی در برابر مداخله فیزیکی و تداخلات محافظت می‌شود. برآورده شدن این مؤلفه‌ها منجر به بسته‌بندی و استفاده توابع امنیتی هدف ارزیابی به صورتی می‌شود که مداخلات فیزیکی قابل تشخیص باشند و یا مجبور به مقاومت در برابر تداخلات فیزیکی شوند. بدون این مؤلفه‌ها، عملکرد حفاظتی از توابع امنیتی هدف ارزیابی اثرشان را در محیط‌هایی که از آسیب فیزیکی نمی‌توان جلوگیری کرد، از دست می‌دهند این خانواده هم‌چنین الزاماتی را ارائه کرده است که چطور توابع امنیتی هدف ارزیابی باید به تلاش‌هایی که در ارتباط با تداخل فیزیکی صورت می‌گیرد واکنش نشان دهند.

- **خانواده بازیابی مطمئن[1]**

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، راه‌اندازی می‌شود و هم‌چنین می‌تواند بازیابی شود. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی، تعیین کننده‌ی حفاظت از وضعیت‌های بعدی است.

- **خانواده تشخیص مجدد[2]**

1 Trusted recovery (FPT_RCV)

2 Replay detection (FPT_RPL)

این خانواده انواع مختلف موجودیت‌ها (به طور مثال، پیغام‌ها، درخواست‌های سرویس، پاسخ‌های سرویس) و اقدامات بعدی را مجدداً تشخیص می‌دهد تا به طور صحیح انجام شده باشند. با توجه به این الزام از مواردی‌که ممکن است مجدداً تشخیص داده شوند به طور موثر جلوگیری می‌شود.

- **خانواده پروتکل هم‌زمانی حالت[1]**

هدف ارزیابی توزیع شده ممکن است نسبت به هدف ارزیابی واحد، به واسطه‌ی اختلاف حالت‌ها بین بخش‌های مختلف هدف ارزیابی و تأخیر در ارتباطات دارای پیچیدگی بیشتر باشد. در اغلب موارد هم‌زمان‌سازی حالت‌ها بین عملکردهای توزیع یافته مستلزم یک پروتکل تبادلی است و یک عمل ساده نیست.

در حالتی‌که عدم اعتماد به محیط توزیع وجود داشته باشد، به پروتکل هم‌زمان‌سازی پیچیده‌تری نیاز است.

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

- **خانواده مهرهای زمانی[2]**

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

---

1 State synchrony protocol (FPT_SSP)

2 Time stamps (FPT_STM)

- **خانواده هم‌خوانی داده‌های بین توابع امنیتی هدف ارزیابی[1]**

در یک محیط توزیعی، هدف ارزیابی ممکن است به تبادل داده توابع امنیتی هدف ارزیابی 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[2]**

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 به سامانه، سرورهای زمانی و غیره) باشد.

- **خانواده هم‌خوانی تکرار داده‌ها در توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی[3]**

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.

---

1 Inter-TSF TSF data consistency

2 Testing of external entities(FPT_TEE)

3 Internal TOE TSF data replication consistency(FPT_TRC)

منظور از هم‌خوانی داده‌ها، یکسان بودن داده‌ها در محل‌ها و توابع مختلف است. داده‌ی توابع امنیتی هدف ارزیابی زمانی ناهم‌خوان می‌شود که کانال داخلی بین بخش‌های 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 بخشهای 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 می شود.

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

چنین خرابی هایی می‌تواند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط در طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهد و 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
۳۱	به روز رسانی امن (FPT_TUD_EXT)	**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 این قابلیت را داشته باشد تا به روزرسانی‌های نرم‌افزار/میان‌افزار هدف ارزیابی را با استفاده از سازوکار امضاء دیجیتال و [انتخاب: درهم‌سازی منتشر شده، هیچ عملکرد دیگر] بررسی کند، پیش از آنکه به‌روزرسانی‌ها نصب شود.
۳۲		**نام عنصر:** خودآزمایی توابع امنیتی هدف ارزیابی۱ **شماره مؤلفه: ح‌ت-خا-(ت‌س).۲,۱ (FPT_TST_EXT.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید مجموعه آزمون‌های خودآزمایی را در طول راه‌اندازی اولیه اجرا کند تا عملکرد صحیح توابع امنیتی هدف ارزیابی را نشان دهد

شماره	نام خانواده	عنصر امنیتی
الزام		
۳۳		**نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی۱**
		شماره مؤلفه: حت-خا-(تس).۲,۱.۱ (FPT_TST_EXT.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید قابلیتی را ارائه دهد تا یکپارچگی و صحت کد اجرایی ذخیره شده توابع امنیتی هدف ارزیابی در زمان بارگذاری برای اجرا از طریق استفاده از سرویس‌های رمزنگاری ارائه شده برای توابع امنیتی هدف ارزیابی که در رز-ع‌ر.۱(۲) مشخص شده است، بررسی و راستی‌آزمایی شوند.
		نکته کاربردی:
		درحالی‌که هدف ارزیابی معمولاً بک بسته نرم‌افزاری است که در محیط IT اجرا می‌شود، با این وجود قادر به اجرای فعالیت‌های خودآزمایی ضروری بالا نیز می‌باشد. در صورت به خطر افتادن محیط میزبان، آزمون خودآزمایی برای برآورده‌سازی امنیت کافی نخواهد بود.
۳۴	به روز رسانی امن	**نام عنصر: به روز رسانی امن ۱**

شماره	نام خانواده	عنصر امنیتی	الزام
			(FPT_TUD_EXT)

شماره مؤلفه: حت-رم-(ت س)۱,۱ **(FPT_TUD_EXT.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به سرپرستان مجاز این قابلیت را بدهند تا بتوانند نسخه فعلی نرم افزار/میان افزار هدف ارزیابی را پرس و جو و مشاهده کنند.

۳۵ **نام عنصر:** به روز رسانی امن ۱

شماره مؤلفه: حت-رم-(ت س)۲,۱ **(FPT_TUD_EXT.1.2)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به سرپرستان مجاز این قابلیت را بدهند تا بتوانند فرآیند به روز رسانی نرم افزار/میان افزار هدف ارزیابی را انجام دهند.

۳۶ **نام عنصر:** به روز رسانی امن ۱

شماره مؤلفه: حت-رم-(ت س)۳,۱ **(FPT_TUD_EXT.1.3)**

شماره **نام خانواده**

عنصر امنیتی

الزام

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به وسیله روشی قبل از به روز رسانی هدف ارزیابی، با استفاده از [انتخاب: سازو کارهای امضای دیجیتال، مقادیر درهم‌سازی منتشر شده] از صحت به روز رسانی نرم افزاری/میان افزاری اطمینان حاصل کنند.

نکته کاربردی:

سازوکار امضاء دیجیتال اشاره به سومین الزام در عنصر رز-ع ر.۱(۲) دارد.

درهم‌سازی منتشرشده توسط یکی از توابع مشخص شده در رز-ع ر.۱(۳) تولید می‌شود.

۷,۶ کلاس کانال/مسیر امن

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 از کانال‌های ارتباطی داخلی و خارجی ساخته شده است که زیر مجموعه مشخصی از داده توابع امنیتی هدف ارزیابی و فرامین را از باقی توابع امنیتی هدف ارزیابی و داده کاربر جداسازی 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 مورد اعتماد بین توابع امنیتی هدف ارزیابی[1]**

1 Inter-TSF trusted channel(FTP_ITC)

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[1]**

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	نام خانواده	عنصر امنیتی
الزام		
۳۷	به روز رسانی امن	**نام عنصر: کانال مورداعتماد داخلی توابع امنیتی هدف ارزیابی ۱**

1 Trusted path(FTP_TRP)

شماره	نام خانواده	عنصر امنیتی
الزام		
(FPT_TUD_EXT)		**شماره مؤلفه: مم-ک‌م.۱,۱ (FTP_ITC.1.1)**
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید کانال ارتباطی امنی را با استفاده از IPsec میان خود و دروازه VPN فراهم کند 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 می‌کند.
۳۸		**نام عنصر: کانال مورداعتماد داخلی توابع امنیتی هدف ارزیابی ۱**
		شماره مؤلفه: مم-ک‌م.۲,۱ (FTP_ITC.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اجازه شروع ارتباط از طریق کانال مورد اعتماد را به توابع امنیتی هدف ارزیابی بدهد.
۳۹		**نام عنصر: کانال مورداعتماد داخلی توابع امنیتی هدف ارزیابی ۱**
		شماره مؤلفه: مم-ک‌م.۳,۱ (FTP_ITC.1.3)

شماره **نام خانواده**

عنصر امنیتی

الزام

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید برای تمام ترافیکی که در آن ارتباط تبادل می‌شود از طریق کانال مورد اعتماد، ارتباطات را آغاز کنند.

نکته کاربردی:

منظور از الزام بالا استفاده از پروتکل‌های رمزنگاری معرفی شده در این الزام، جهت محافظت ارتباط بین هدف ارزیابی و دروازه VPN است.

این الزام دلالت برآن دارد که حتی پس از قطع ارتباط محافظت از سر گرفته شود.

۸ الزامات تضمین امنیتی

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

۸,۱ کلاس توسعه

اطلاعات در رابطه با هدف‌های ارزیابی منطبق بر این پروفایل حفاظتی، در «مستندات راهنما» یا بخش «مشخصات امنیتی هدف ارزیابی[1]» سند هدف امنیتی لحاظ شده است و در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی هدف ارزیابی» در سند هدف امنیتی نیست، اما در صورت وجود باید محتوای آن مرتبط با الزمات کارکردی و مورد تائید توسعه دهندگان هدف ارزیابی باشد.

فعالیت‌های تضمینی که در بخش «الزامات تضمین» آمده است باید به نویسندگان سند هدف امنیتی اطلاعات کافی بدهند تا آنها بتوانند برای بخش «مشخصات امنیتی هدف ارزیابی» محتوای مناسبی را در نظر بگیرند.

در زمینه درک و فهم واسط‌ها به هدف ارزیابی، مهم در نظر گرفتن تهدیدهایی است که با محرمانگی و صحت داده‌های کاربری که در میان شبکه منتقل می‌شوند یا داده‌های احراز هویتی که ممکن است پیمایش کننده اتصال باشد، مقابله می‌کنند (از طریق اتصالات یک به یک هدف ارزیابی یا اتصال هدف ارزیابی به VPN Gateway). هم‌چنین هدف ارزیابی با توجه به پیکربندی‌اش، ممکن است پیشنهاد حفاظت از دسترسی غیرمجاز به شبکه پشت هدف ارزیابی کند. علاوه بر واسط‌های شبکه لازم است که واسط‌های سرپرستی (چگونه هدف ارزیابی پیکربندی می‌شود) شرح داده شوند.

1 TOE Security Specification

۸,۱,۱ مشخصات کارکردی

مشخصات کارکردی، واسطهای کارکرد امنیتی هدف ارزیابی را توصیف می‌کند اما نیازی به شرح مفصل و کاملی از این واسطها نیست. فعالیت‌های این خانواده باید بر روی درک پاسخ واسطهای ارائه شده در دو بخش «مشخصات امنیتی هدف ارزیابی» و «مستندات راهنما» به الزامات کارکردی متمرکز شود.

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

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		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، هستند. با توجه به دلایلی که باید در مستندات و بخش "خلاصه مشخصات هدف ارزیابی" وجود داشته باشند. 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 نیست.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **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] را توصیف کند.
۴		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2C)**

1 SFR-enforcing TSFI

2 SFR-supporting TSFI

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص کند.
۵		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.3C)** **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه کند.
۶		**نام عنصر: مشخصات کارکرد ابتدایی۱**

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (ADV_FSP.1.4C) **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطه‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.
۸		**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 هستند.

۸,۲ کلاس راهنمای کاربر

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

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

- دستورالعمل نصب موفقیت آمیز هدف ارزیابی در محیط
- دستورالعمل مدریت امنیت هدف ارزیابی به عنوان یک محصول یا به عنوان بخشی از یک محیط عملیاتی بزرگتر
- دستورالعمل‌هایی که ارائه دهنده قابلیت سرپرستی محافظت شده از طریق استفاده از قابلیت‌های هدف ارزیابی، محیط عملیاتی یا هر دو هستند.

۸,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۹	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
۱۰	راهنمای کاربردی (AGD_OPE)	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را کـه بایـد در یـک محیط پردازشی امن کنترل شوند توصیف کند، مانند هشدارهای مناسب.
۱۱		**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

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شده توسط هدف ارزیابی به صورت امن استفاده می‌شود.
۱۲		**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 و مقادیر امن را به صورت مناسبی تعیین کند.
۱۳		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		در دسترس کاربر که نیاز است انجام شوند، مرتبط کند، مانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی هدف ارزیابی.
۱۴		**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 الزامشان را برای حفظ عملیات در حالت امن مشخص کند.
۱۵		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده است، کاملاً اجرا شوند.
۱۶		**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
۱۷	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**
۱۸	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (AGD_PRE.1.1D) **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۹	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:**

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

مؤلفه‌های اقدامات ارزیاب

مؤلفه‌های اقدامات ارزیاب		
۲۱	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.
۲۲		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید کند هدف ارزیابی می‌تواند به صورت امن برای عمل کردن 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 است 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**
۲۳	آزمون مستقل	**نام عنصر: آزمون مستقل ۱**

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

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

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		هدف ارزیابی باید مناسب آزمون باشد.

مؤلفه‌های اقدامات ارزیاب		
۲۵	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.
۲۶		**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
		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 کردن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی آن دسته از آسیب‌پذیری‌هایی را که در این نوع محصولات یافت شده‌اند بیابند. 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 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**
۲۷	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمون ، هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۸	آسیب‌پذیری	**نام عنصر: آسیب‌پذیری ۱**

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

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۹	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۳۰		**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.
۳۱		**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

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		ارزیابی را 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 برچسب گذاری هدف ارزیابی

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

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۲	قابلیت‌های پیکربندی	**نام عنصر: برچسب‌گذاری هدف ارزیابی ۱**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
	(ALC_CMC)	**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**
۳۳	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		هدف ارزیابی باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۴	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
۳۵	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

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۶	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.
۳۷		**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**
۳۸	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.