به نام خدا

پروفایل حفاظتیVPN GateWay

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 GateWay می‌باشد تا تولیدکنندگان این دسته از محصولات 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 محصول VPN GateWayبه 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 می‌گردد.

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

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 محصولات VPN GateWay در این سند مطرح شده است عبارتند از:

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس شناسایی و احراز هویت

- کلاس مدیریت امنیت
- کلاس حفاظت ازتوابع امنیتی هدف ارزیابی
- کلاس فیلترنمودن بسته‌ها
- کلاس کانال‌ها / مسیرهای مورد اعتماد

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.

محصول VPN GateWay تمام کلاس‌هایی که در «سند پروفایل حفاظتی تجیهزات شبکه» مطرح شده است را در بر می‌گیرد (اعم از کلاس های کارکرد امنیتی و تضمین امنیتی) علاوه بر آن دارای کلاس‌هایی می‌باشد که در این سند معرفی شده است.

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 که در این سند برای برآورده نمودن 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.

- **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.

[1] Protection Profile

[2] Security Target

- **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.

- **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 می‌نماید.

این بیانیه شامل موارد زیر است:

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

- **عامل تهدید (Threat Agent)**

موجودیت‌هایی که می‌توانند بر روی دارایی‌ها اقدام تهاجمی انجام دهند.

- **خط‌مشی امنیتی سازمانی (OSP[2])**

[1] Non-Target Of Evaluation

[2] Organizational Security Policy

مجموعه‌ای از قوانین، که توصیف کننده رفتار امنیتی خاصی است که توسط «توابع امنیتی هدف ارزیابی» اجرا می‌گردند؛ 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 تهدیدهای معرفی شده و/یا برای برآورده نمودن 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 می‌گردند تا در حاصل شدن اهداف ارزیابی، برای هدف ارزیابی کمک نمایند.

- **الزام کارکرد امنیتی (SFR[1])**

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.

- **الزامات تضمین امنیتی (SAR[2])**

این دسته از الزامات اطمینان می‌دهند که الزامات کارکرد امنیتی توسط هدف ارزیابی برآورده می‌گردند. 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.

[1] Security Functional Requirement

[2] Security Assurance Requirement

- **سطح تضمین ارزیابی (EAL[1])**

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» می-باشد.

- **توابع امنیتی هدف ارزیابی (TSFs[2])**

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)**

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)**

[1] Evaluation Assurance Level

[2] TOE Security Functions

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 می-باشد.

- **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 مولفه‌های قابل انتخاب، که الزامات ممکن است براساس آن‌ها باشد.

- **مولفه (Element)[۲]**

بیانی از نیاز امنیتی که غیر قابل تجزیه است.

- **اختصاص (Assignment)**

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

- **انتخاب (Selection)**

[۱] در استاندارد ISO 15408 منتشر شده توسط سازمان استاندارد، Component مولفه ترجمه شده است.

[۲] در استاندارد ISO 15408 منتشر شده توسط سازمان استاندارد، Element عنصر ترجمه شده است.

انتخاب نمودن یک یا بیش از یک آیتم در لیستی که در مولفه 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 و یا اطلاعات را دریافت می‌نماید 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 گردد.

- **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 می‌شوند.

- **خط‌مشی کارکرد امنیتی (SFP[1])**

رفتار امنیتی که توسط «کارکرد امنیتی هدف ارزیابی» اجرا می‌گردد 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 نماید، 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 نماید. تمام این خط‌مشی‌ها توسط «توابع امنیتی هدف ارزیابی» پیاده‌سازی می‌شوند.

- **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.

[1] Security Functionality Policy

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

«خط‌مشی کنترل 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 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، می‌باشد.

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

---

[1] Common Criteria (CC)

[2] Protection Profile (PP)

[3] Security Target (ST)

[4] Target Of Evaluation (TOE)

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

بخش دوم: الزامات کارکرد امنیتی [۱]

بخش سوم: الزامات تضمین امنیتی [۲]

۴ معرفی گذرگاه VPN[۳]

این بسته توسعه یافته به تجهیزات گذرگاه شبکه اشاره می‌کند که تونل‌های VPN پروتکل IPsec را پایان می‌دهد. گذرگاه VPN که منطبق این سند است، ابزاری تشکیل شده از سخت‌افزار و نرم‌افزاری است که به دو یا بیش از دو شبکه مجزا متصل بوده و نقش زیر ساختی در تشکیلات کلی شبکه دارد. به طور خاص، گذرگاه VPN تونل امنی را ایجاد می‌نماید که مسیر رمز شده و احراز هویت شده به دیگر سایت‌ها را فراهم می‌نماید و بدین وسیله خطر افشای اطلاعاتی که به شبکه ناامن منتقل می‌شود را کاهش می‌دهد.

[1] Security Functional Requirement (SFR)

[2] Security Assurance Requrement (SAR)

[3] VPN Gateway

لذا این بسته توسعه یافته بر روی پروفایل حفاظتی مربوط به تجهیزات شبکه ایجاد شده است، هدف‌های ارزیابی که مطابق این پروفایل حفاظتی باشند، متعهد هستند که عملکرد لازم در پروفایل حفاظتی مربوط به تجهیزات شبکه همراه با عملکردهای اضافی که در این بسته توسعه یافته تعریف شده است را پیاده‌سازی نمایند تا با تهدیدهای امنیتی، مقابله نمایند.

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

۵ تعریف مسائل امنیتی

۵,۱ فرضیات

A.TYPE	توضیحات
A.CONNECTIONS	فرض می‌شود که هدف ارزیابی به گونه‌ای به شبکه‌های جداگانه متصل می‌گردد که از قابل اجرا بودن خط‌مشی-های امنیتی هدف ارزیابی بر روی تمام جریان ترافیک شبکه در بین شبکه‌های متصل اطمینان حاصل نماید.

۵,۲ تهدیدها

T.TYPE	توضیحات
T.NETWORK_DISCLOSURE	اطلاعات حساس بر روی یک شبکه محافظت شده ممکن است در نتیجه اقدامات مبتنی بر دخول یا خروج

T.TYPE	توضیحات
	افشاء گردد.[1]
T. NETWORK_ACCESS	ممکن است از خارج شبکه محافظت شده به سرویس‌های درون شبکه یا متناوباً ازداخل شبکه محافظت شده به سرویس‌های خارج شبکه، به دسترسی غیرمجاز دست یافت.
T.NETWORK_MISUSE	دستیابی به سرویس‌هایی که توسط یک شبکه محافظت شده در دسترس قرار گرفته‌اند ممکن است در مقابل خط‌مشی‌های محیط عملیاتی استفاده شوند.
T.TSF_FAILURE	در صورت شکست خوردن سازوکارهای امنیتی هدف ارزیابی، عملکرد امنیتی هدف ارزیابی نیز به خطر می‌افتد.
T.REPLAY_ATTACK	اگر موجودیت IT خارجی یا مخرب بتواند به شبکه دستیابی داشته باشد، ممکن است توانایی ربودن اطلاعات در حرکت در سراسر شبکه و فرستادن آنها به مقصد مورد نظر را نیز داشته باشد.
T.DATA_INTEGRITY	بخش مخربی که سعی در تغییر داده فرستاده شده دارد سبب از بین رفتن صحت داده می‌شود.

۵,۳ خط‌مشی‌ها

هیچ خط‌مشی در این بخش معرفی نشده است.

[1] Ingress or egress-based actions

۶ اهداف امنیتی

۶,۱ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.ADDRESS_FILTERING	هدف ارزیابی توانایی فیلتر نمودن و گزارش‌گیری بسته‌های شبکه را براساس آدرس مبدا و مقصد فراهم خواهد نمود.
O.AUTHENTICATION	هدف ارزیابی توانایی احراز هویت کاربران را ارائه خواهد نمود تا اطمینان دهند که آنها با موجودیت IT خارجی مجازی در ارتباط هستند.
O.CRYPTOGRAPHIC_FUNCTIONS	هدف ارزیابی توانایی رمزنگاری و رمزگشایی داده را ارائه خواهد نمود تا محرمانگی حفظ گردد و اجازه می-دهد تا داده‌های عملکرد امنیتی هدف ارزیابی که خارج از هدف ارزیابی منتقل می‌گردند تغییر شکل یابند (رمز شوند) و آشکار گردند (رمزگشایی گردند).
O.FAIL_SECURE	هنگامیکه خودآزمایی با شکست مواجه می‌گردد، هدف ارزیابی خاموش خواهد شد تا اطمینان حاصل شود که داده‌ها نمی‌توانند منتقل گردند.
O.PORT_FILTERING	هدف ارزیابی توانایی فیلتر نمودن و گزارش‌گیری بسته‌های شبکه را براساس پورت‌های لایه انتقال مبدا و مقصد فراهم خواهد نمود.

۶,۲ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.CONNECTIONS	سرپرستان هدف ارزیابی اطمینان خواهند داد که هدف ارزیابی به صورتی نصب می‌گردد که اجازه خواهد داد خط‌مشی‌های هدف ارزیابی بر روی جریان ترافیک شبکه در میان شبکه‌های متصل شده، اجرا گردد.

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 خواهند داشت.

شماره آیتم	نام کلاس	الزام	نام الزام
۱	کلاس ممیزی(FAU)	FAU_GEN.1	تولید داده ممیزی
۲	کلاس پیشتیبانی از رمزنگاری (FCS)	FCS_CKM.1	مدیریت کلید رمزنگاری
		FCS_COP.1	عملیات رمزنگاری
		FCS_RBG.1	تولید بیت تصادفی
		FCS_IPsec	پروتکل IPsec
۳	کلاس شناسایی و احرازهویت (FIA)	FIA_X509_EXT.1	خانواده گواهینامه X509
		FIA_AFL.1	اداره نمودن شکست در احرازهویت
۴	کلاس مدیریت امن (FMT)	FMT_MOF.1	مدیریت رفتار توابع امنیتی
		FMT_SMF.1	مشخصات عملکردهای مدیریتی
۵	کلاس حفاظت از توابع امنیتی هدف ارزیابی (FPT)	FPT_TUD.1	بروزرسانی امن
		FPT_TST.1	خودآزمایی توابع امنیتی هدف ارزیابی
۶		FPT_FLS.1	نقض امنیت

شماره آیتم	نام کلاس	الزام	نام الزام
۷	کلاس فیلتر نمودن بسته‌ها (FPF)	FPF_RUL.1	فیلتر نمودن بسته‌ها
۸	کلاس کانال‌ها/مسیرهای مورد اعتماد (FTP)	FTP_ITC.1	کانال مورد اعتماد بین توابع امنیتی هدف ارزیابی

۷,۱ کلاس ممیزی امنیت[1]

نام کلاس: ممیزی امنیت

شرح کلاس: سامانه‌های VPN Gateway برای رخدادهای گوناگون اقدام به ایجاد گزارش‌هایی برای ممیزی می‌نمایند. کلاس ممیزی امنیت، الزاماتی پیرامون نحوه شناخت، ثبت و ذخیره و آنالیز اطلاعات ممیزی مربوط به فعالیت‌های امنیتی تعریف نموده است (فعالیت‌هایی که توسط توابع امنیتی هدف ارزیابی کنترل می‌گردند). با بررسی ممیزی‌های ثبت شده می‌توان تعیین کرد که کدام رخداد مرتبط با چه فعالیت امنیتی صورت گرفته و چه‌کسی (چه کاربری) مسوول آن است. این کلاس شامل شش خانواده است که عبارتند از:

- **خانواده پاسخ پاسخ خودکار ممیزی امنیت[2]**

[1]Security audit (Class FAU)

[2]Security audit automatic response (FAU_ARP)

این خانواده تعریف کننده الزامات برای واکنش‌های سیستم نسبت به رویدادهایی است که به‌روز بودن آنها نشان‌دهنده نقض امنیتی بالقوه‌ای باشد.

- **خانواده تولید داده ممیزی[1]**

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

- **خانواده تحلیل ممیزی امنیت[2]**

این خانواده الزاماتی برای ابزارهای خودکار، که فعالیت‌های سیستم را تحلیل می‌نماید و داده‌های ممیزی که نقض امنیتی واقعی یا ممکن را جستجو می-کنند، تعریف می‌نماید. این تحلیل ممکن است در پشتیبانی از تشخیص نفوذ، یا پاسخ خودکار به نقض امنیتی بالقوه کار نماید.

- **خانواده بازبینی ممیزی امنیت[3]**

[1]Security audit data generation(FAU_GEN)

[2]Security audit analysis (FAU_SAA)

[3]Security audit review (FAU_SAR**)**

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

- **خانواده انتخاب رویداد ممیزی امنیت[1]**

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

- **خانواده ذخیره‌سازی رویداد ممیزی امنیت[2]**

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

در کلاس ممیزی امنیت، نسبت به پروفایل حفاظتی NDPP الزامات بیشتری تعریف شده است، که عبارتند از:

شماره نام خانواده نام مولفه

[1]Security audit event selection (FAU_SEL)

[2]Security audit event storage (FAU_STG)

الزام

۱ **نام عنصر: تولید داده ممیزی امنیت ۱**

شماره مولفه:ما-ت‌ل.۱ (FAU_GEN.1)

شرح مولفه:

شرح مولفه مطابق با شرح آن در مستند مرتبط با تجهیزات شبکه است با این تفاوت که رویدادهای قابل ممیزی زیادی وجود دارد که برای توسعه الزام عملکرد امنیتی ما-ت‌ل.۱ در NDPP باید به آن اضافه گردد. لذا، رویدادهای زیر باید با آن دسته رویدادهای قابل ممیزی NDPP اضافه شده و رویدادهای ممیزی زیر برای این EP[1] لازم و ضروری است.

تولید داده ممیزی امنیت.

(FAU_GEN.1)

الزام	رویداد قابل ممیزی	محتویات رکورد ممیزی اضافی
رز-اپ-(ت‌س).۱	ایجاد نشست با همدیگر	آدرس مبدا و مقصد پورت مبدا و مقصد واسط هدف ارزیابی
اش-X509-(ت‌س).۱	ایجاد نشست یا CA[2]	آدرس مبدا و مقصد

[1]Extended Package

[2]Certification Authority

		پورت مبدا و مقصد واسط هدف ارزیابی
ف‌ب-ف‌ت-(ت‌س).۱	بکارگیری قوانینی که با عملکرد «گزارش‌گیری»پیکربندی شده باشند	آدرس مبدا و مقصد پورت مبدا و مقصد پروتکل لایه انتقال واسط هدف ارزیابی
	نشان دادن دور انداختن بسته‌ها به علت ترافیک زیاد شبکه	واسط شبکه که قادر به پردازش بسته‌ها نمی‌باشد

نکته کاربردی:

برای نشست ایجاد شده، انتظار می‌رود که هدف ارزیابی قادر به ممیزی نمودن تمام بسته‌های مرتبط با نشست ایجاد شده باشد؛ این شامل فاز ۱ IKE و فاز ۲ مذاکرات است. هدف ارزیابی باید قادر به گزارش‌گیری از تمام بسته‌ها در نشستی که به صورت موفقیت آمیز ایجاد شده است باشد، هم‌چنین قادر به گزارش‌گیری از هر بسته‌ای باشد که رد و یا دور انداخته شده است.

۷,۲ کلاس پشتیبانی از رمزنگاری[1]

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 می‌توانند شامل موارد زیر باشند، اما تنها به این دسته نیز محدود نمی‌گردند:

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

این کلاس زمانی‌که هدف ارزیابی، عملکرد رمزنگاری را پیاده‌سازی می‌نماید، استفاده می‌شود این پیاده‌سازی می‌تواند در نرم‌افزار، سخت‌افزار و میان افزار

[1]Cryptographic Support(Class FCS)

صورت گیرد.

➢ خانواده مدیریت کلید رمزنگاری[1]

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

- 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]

به منظور عملکرد صحیح عملیات رمزنگاری، این عملیات باید مطابق با الگوریتم خاص و کلید رمزنگاری با اندازه مشخص انجام گیرد. در صورت وجود

[1]Cryptographic key management(FCS_CKM)

[2]Cryptographic operation(FCS_COP)

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 و یا تائید کنترل، درهم‌سازی امن (خلاصه پیام)، رمزنگاری و/یا رمزگشایی کلید رمزنگاری و توافق کلید رمزنگاری می‌باشد.

شماره الزام	نام خانواده مولفه امنیتی
۲	**نام عنصر: مدیریت کلید رمزنگاری ۱ (۱)** **شماره مولفه: رز-م‌ک.۱,۱ (FCS_CKM.1.1)**
تولید کلید رمزنگاری (FCS_CKM)	**شرح مولفه:** توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری نامتقارن که برای ایجاد کلید استفاده می‌شوند را مطابق با • استاندارد NIST SP 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته» برای طرح برقراری کلید متناهی مبتنی بر میدان[1]

[1]checksum

شماره نام خانواده

مولفه امنیتی

الزام

- استاندارد NIST 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته[۲]» برای برقراری طرح کلید مبتنی بر منحنی بیضوی[۳] و پیاده‌سازی «NIST Curves»در P-256 و P-384 و [انتخاب:*P-521*، هیچ منحنی دیگری](چنان‌که در FIPS PUB 186-3،«استاندارد امضایدیجیتال»تعریف شده است)
- [انتخاب:

استاندارد NIST SP 800-56 B، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری تجزیه عدد صحیح[۴]برای طرح برقراری کلید مبتنی بر RSA.»]

تولید نمایند. همچنین اندازه این کلید باید معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد.

نکته کاربردی:

این بسته توسعه یافته ملزم می‌نماید تا از الگوریتم‌های خاص به منظور ایجاد کلید استفاده گردد. این مولفه هدف ارزیابی را قادر می‌سازد

---

[1] Field-bsae

2 Discrete Logarithm Cryptography”

3Curve-base

4Integer Factorization Cryptography

شماره	نام خانواده	مولفه امنیتی
		الزام
		تا برای پروتکل‌های مختلف رمزنگاری (برای مثالIPsec) که توسط هدف ارزیابی استفاده می‌گردند، جفت کلید عمومی/خصوصی تولید نمایند.
		از آنجا که پارامترهای دامنه مورد استفاده، توسط الزامات پروتکل در پروفایل حفاظتی مشخص شده‌اند، نیازی به اعتبار سنجی آنها زمانی‌که هدف ارزیابی با پروتکل تعریف شده در این پروفایل حفاظتی مطابقت دارد، نمی‌باشد.
۳	عملیات رمزنگاری (FCS_COP)	**نام عنصر: عملیات رمزنگاری(برای رمزنگاری/رمزگشایی داده) ۱ (۱)**
		شماره مولفه:رز-ع‌ر.۱,۱ (۱)((FCS_COP.1.1(1))
		شرح مولفه:
		توابع امنیتی هدف ارزیابی باید [**رمزنگاری و رمزگشایی**] را مطابق با الگوریتم رمزنگاری AESکه در مود**CBC**، **GCM**،[اختصاص: **یک یا بیش از یک مود، هیچ مود دیگر**] عمل می‌کند و اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی و [انتخاب:*۱۹۲ بیتی، نه هیچ اندازه دیگری*]مطابق با استاندارد: – استانداردFIPS PUB 197 – NIST SP 800-38D ،NIST SP 800-38A – [انتخاب: *NIST SP 800-38B, NIST SP 800-38C NIST SP 800-38E , هیچ استاندارد دیگر*] انجام بدهند.

شماره	نام خانواده	مولفه امنیتی
الزام		

نکته کاربردی:

این بسته توسعه یافته 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). بنابراین مولفه رز-ع‌ر.۱,۱(۱) در NDPP مشخص شده در اینجا اطمینان می‌دهد که نویسنده هدف امنیتی شامل این دو مود می‌باشد تا با الزامات IPsec سازگار باشد.

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

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید خدمات رمزنگاری امضا را مطابق با موارد زیر انجام دهند:

[انتخاب :

- الگوریتم امضای دیجیتال RSA (rDSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با FIPS PUB 186-2یا FIPS PUB 186-3،«استاندارد امضای دیجیتال»

شماره	نام خانواده	مولفه امنیتی
الزام		
		• الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA[1]) با کلید ۲۵۶ بیتی یا بیشتر مطابق با ○ FIPS PUB 186-3 ، «استاندارد امضای دیجیتال» تابع ارزیابی امنیتی باید «منحنی‌های استانداردNIST curves»،P-256،P384 و [انتخاب : P251 ، نه سایر منحنی‌ها] (هم‌چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده‌است)]
۵		**نام عنصر:** تولید بیت تصادفی۱
		شماره مولفه:رز-ب‌ت.۱,۱ (FCS_RBG.1.1)
تولید بیت تصادفی(ت‌س) **(FCS_RBG_EXT)**		**شرح مولفه:** 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)، CTR_DRBG (AES)، Dual_EC_DRBG (هرکدام)]، پیوست C استاندارد FIPS Pub 140-2؛ ضمیمه ۲,۴ از استاندارد X9.31 با استفاده از الگوریتمAES*]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*

[1]Elliptic Curve Digital Signature Algorithm

شماره نام خانواده

الزام

مولفه امنیتی

توابع امنیتی هدف ارزیابی] محاسبه می‌گردد.

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 یاپیوستC استاندارد FIPS.)

استاندارد90-SP800 در برگیرنده 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 نمود(اگر 90-800 انتخاب شده باشد) همچنین اصول اولیه رمزنگاری استفاده شده را با اضافه نمودن الزام یا در بخش خلاصه امنیتی هدف ارزیابی لحاظ می‌نماید.

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 SP800-90 مجاز هستند، نویسنده هدف امنیتی باید در سند هدف امنیتی منحنی و الگوریتم درهم‌ساز استفاده شده را لحاظ نماید.

در دومین انتخاب این الزام، نویسنده هدف امنیتی مشخص می‌نماید که منبع آنتروپی مبتنی بر نرم‌افزار است یا سخت‌افزار یا هردو.

شماره	نام خانواده	مولفه امنیتی
الزام		

اگر چند منبع آنتروپی وجود داشته باشد، نویسنده هدف امنیتی باید به طور دقیق منبع هر آنتروپی را مشخص نماید که مبتنی بر سخت‌افزار است یا نرم‌افزار. به طور کلی اولویت با منابع نویز مبتنی بر سخت‌افزار است.

توجه داشته باشید که در پیوست C استاندارد FIPS140-2، در حال حاضر تنها روش شرح داده شده در توصیهNIST، تولید کننده عددتصادفی مبتنی بر پیوست الف.۲,۴ از ANSIX9.31 با استفاده از سه کلید سه‌تایی الگوریتم‌های DES و AES[1]در بخش ۳، معتبر می-باشند.

در صورتی که طول کلید استفاده شده در پیاده‌سازی AES با طول کلید استفاده شده در رمزنگاری داده متفاوت باشد، آنگاه باید الزام (رز-ع‌ر.۱) را برای منعکس نمودن طول کلید متفاوت، دو بار تکرار نمود.

در کلاس رمزنگاری، علاوه بر الزامات مطرح شده در NDPP، الزامات جدیدی برای VPN Gateway در نظر گرفته شده است:

شماره	نام خانواده	عنصر امنیتی
الزام		

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

۱ مدیریت کلید رمزنگاری (FCS_CKM)

نام عنصر: مدیریت کلید رمزنگاری ۱ (۲)

شماره مولفه: رز-م‌ک.۱,۲ (FCS_CKM.1.2)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری نامتقارن مورد استفاده احراز هویت همتای IKE مطابق با انتخاب-های زیر را تولید نمایند:

[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-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر]
- ANSI X9.31-1998، پیوست A.2.4 با استفاده از AES برای طرحRSA]

و اندازه‌های کلید رمزنگاری شده معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی.

نکته کاربردی:

در قسمت انتخاب این الزام، استانداردANSI X9.31-1998 در نسخه‌های بعدی این پروفایل حفاظتی حذف خواهد شد. در حال حاضر انتخاب به FIPS PUB 186-3 محدود نشده است تا به صنعت ، زمان بیشتری داده شود تا بطور کامل از استاندارد مدرن FIPS PUB 186-3 استفاده نمایند.

کلیدهایی که لازم است توسط هدف ارزیابی از طریق این الزام تولید گردند، برای احراز هویت همتای VPN در طول تبادلات کلید IKE (v1یا v2)استفاده می‌شوند . در حالی‌که این الزام کلید عمومی را ملزم می‌نماید با یک شناسه در گواهینامه X509v3 مرتبط گردد، ضرورتی ندارد که این مرتبط شدن توسط هدف ارزیابی صورت بگیرد، انتظار می‌رود که این امر توسط مرکز صدور گواهینامه در محیط عملیاتی انجام گردد.

همان‌گونه که در الزام رز-اپ-(ت‌س).۱ نشان داده شده است، هدف ارزیابی جهت احراز هویت همتا ، ملزم به پیاده-سازی RSAیا ECDSA (یا هردو) می‌باشد. اندازه‌های کلید تولید شده از کلیدهای ۲۰۴۸بیتی RSA باید معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد. همان طور که در NIST SP 500-57، «پیشنهاداتی برای مدیریت کلید» اطلاعاتی مرتبط با قدرت کلیدِ معادل، آورده است.

۲ پروتکل Ipsec (FCS-IPsec(EXT))

نام عنصر: پروتکلIPsec ۱

شماره مولفه: رز-اپ-(ت‌س).۱,۱ (FCS_IPSEC_EXT.1.1)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید معماری IPsec به صورت مشخص شده در RFC 4301 را پیاده‌سازی نمایند.

۳ **نام عنصر: پروتکلIPsec ۱**

شماره مولفه: رز-اپ-(ت‌س).۲,۱ (FCS_IPSEC_EXT.1.2)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید [انتخاب: مود تونل، مود انتقال] را پیاده‌سازی نمایند.

نکته کاربردی:

نسخه‌های بعدی این بسته توسعه یافته، توابع امنیتی هدف ارزیابی را ملزم به استفاده از هر دو مود(تونل و انتقال) می-نمایند.

۴ **نام عنصر: پروتکلIPsec ۱**

شماره مولفه: رز-اپ-(ت‌س).۳,۱ (FCS_IPSEC_EXT.1.3)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید در انتهای لیست پایگاه داده خط مشی‌های 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 گردد.

۵ **نام عنصر: پروتکلIPsec ۱**

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید ESP پروتکل IPsec را به صورت تعریف شده در RFC 4303 و با استفاده از الگوریتم‌های

[1]-Security policy database

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] را پیاده‌سازی نمایند.

نکته کاربردی:

در صورت انتخاب AES-CBC، الگوریتم درهم‌سازی امن مبتنی بر HMAC باید با آنچه که در NDPP عنصر عملیات رمزنگاری رز-ع‌ر.۱(۴) مشخص شده است، سازگار باشد.

نام عنصر: پروتکلIPsec ۱ ۶

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

شرح مولفه:

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 درRFC 5996و [انتخاب: هیچ RFC دیگری برای عملیات درهم‌سازی، RFC 4868 برای عملیات درهم‌سازی] را پیاده‌سازی نمایند.

نام عنصر: پروتکلIPsec ۱

۷

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که سرآیند[1] رمزنگاری شده در پروتکل [انتخاب: IKE1،] IKE2، الگوریتم‌های رمزنگاریAES-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] را استفاده می‌نمایند.

[1]-Payload

توابع امنیتی هدف ارزیابی باید معماری IPsec به صورت مشخص شده در RFC 4301 را پیاده‌سازی نمایند.

۸ **نام عنصر: پروتکلIPsec ۱**

شماره مولفه: رز-اپ-(ت‌س).۷,۱ (FCS_IPSEC_EXT.1.7)

شرح مولفه:

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

نکته کاربردی:

این مولفه تنها زمانی قابل اجرا می‌باشد که IKEv1 انتخاب گردد.

۹ **نام عنصر: پروتکلIPsec ۱**

شماره مولفه: رز-اپ-(ت‌س).۸,۱ (FCS_IPSEC_EXT.1.8)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که

[انتخاب:

- دوره حیاتSA مربوط به IKEv2 می‌تواند توسط سرپرست براساس تعداد بسته یا بازه زمانی پیکربندی گردد، بطوریکه بازه زمانی محدود باشد به: ۲۴ ساعت برای فاز۱ SA و ۸ ساعت برای فاز ۲ SA،
- دوره حیاتSA مربوط به IKEv1 می‌تواند توسط سرپرست براساس تعداد بسته یا بازه زمانی پیکربندی گردد، بطوریکه بازه زمانی محدود باشد به: ۲۴ ساعت برای فاز۱ SA و ۸ ساعت برای فاز ۲ SA]

نکته کاربردی:

مطلوب است که این الزام به جای تعداد بسته‌ها از عددی برحسب Mb/Kb استفاده نماید، به شرط آنکه هدف ارزیابی قادر باشد محدودیتی بر روی میزان ترافیکی که توسط همان کلید محافظت می‌گردد، اعمال نماید.

نام عنصر: پروتکلIPsec ۱ ۱۰

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید مقدار رمز x را تولید نمایند که در تبادلات کلید الگوریتم Diffie-Hellman پروتکل IKE استفاده می‌گردد، این مقدار x با استفاده از عنصر تولید بیت تصادفی که در قسمت رز-بت-(تس).۱ مشخص شده است، تولید می‌گردد. 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.

نام عنصر: پروتکلIPsec ۱ ۱۱

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید عدد تصادفی(nonce) را تولید نمایند که در تبادلات IKE استفاده می‌شود به طوریکه احتمال تکرار این عدد در دوره حیات SA مربوط به پروتکل IPsec کمتر از ۱ در ۲[^ 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.

۱۲ **نام عنصر: پروتکلIPsec ۱**

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE گروه‌های Diffie-Hellman۱۴(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: دیگر گروه‌های DH که توسط هدف ارزیابی پیاده‌سازی شده‌اند]، هیچ گروه DH دیگر] را پیاده‌سازی می‌نمایند.

۱۳ **نام عنصر: پروتکلIPsec ۱**

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

شرح مولفه:

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

۱۴ **نام عنصر: پروتکلIPsec ۱**

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

شرح مولفه:

توابع امنیتی هدف ارزیابی باید بتوانند به صورت پیش‌فرض اطمینان دهند که الگوریتم متقارن پیشنهاد شده جهت حفاظت اتصال [انتخاب: فاز ۱ IKEv1، IKE_SA IKEv2] از نظر قدرت بزرگتر یا معادل الگوریتم متقارن (تعداد بیت-های کلید) پیشنهاد شده جهت حفاظت اتصال [انتخاب: فاز ۲ IKEv1، CHILD_SAIKEv2] می‌باشند.

۷,۳ کلاس شناسایی و احراز هویت[1]

در ادامه المان‌های امنیتی مورد نیاز کلاس شناسایی و احرازهویت ارائه شده است.

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 نمودن لازم و ضروری می‌باشد تا تضمین شود که کاربران همراه با صفات امنیتی مناسبی می‌باشند (به طور مثال، هویت، گروه‌ها، نقش‌ها، سطوح یکپارچگی یا امنیت)

شناسایی غیر مبهم کاربران مجاز و اختصاص صحیح صفات امنیتی به کاربران و موجودیت‌های فعال بسیار مهم و حساس است تا خط مشی‌های 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 را تعیین نمایند، و برای هر کاربر مجاز مشخصه‌های امنیتی را 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[2]**

[1]Identification and authentication (Class FIA)

[2]Authentication failures(FIA_AFL)

این خانواده حاوی الزاماتی است که تعریف کننده مقادیری برای تعداد تلاش‌های ناموفق صورت گرفته جهت احراز هویت می‌باشد، هم‌چنین اقداماتی که توابع امنیتی هدف ارزیابی در مواردی که تلاش جهت احراز هویت با شکست مواجه می‌گردد را تعریف می‌نماید. پارامترهایی هم‌چون تعداد تلاش‌های احراز هویت منجر به شکست و آستانه زمان در الزامات این خانواده تعیین می‌گردد.

- **خانواده تعریف مشخصه کاربر[1]**

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 نمودن مشخصه‌های امنیتی کاربر به کاربران تعریف می‌نماید تا در صورت لزوم توابع امنیتی هدف ارزیابی را در تصمیم‌گیری های امنیتی پشتیبانی نماید.

- **خانواده خصوصیات رازها[2]**

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

- **خانواده احراز هویت کاربر[3]**

[1]User attribute definition (FIA_ATD)

[2]Specification of secrets (FIA_SOS)

[3]User authentication (FIA_UAU)

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

- **خانواده شناسایی کاربر[1]**

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 می-باشند.

- **خانواده اتصال موجودیت فعال- کاربر[2]**

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 می‌گردد (به طور کامل یا بخشی از آن). این خانواده الزاماتی را تعریف می‌نماید تا ایجاد و نگهداری ارتباط بین کاربر و موجودیت فعال متناظر با آن را فراهم آورد.

در این کلاس شناسایی و احراز هویت نسبت به NDPP الزامات بیشتری تعریف شده است، که در ادامه آورده شده است:

شماره الزام	نام خانواده	مولفه امنیتی

[1]User identification (FIA_UID)

[2]User – subject binding (FIA_USB)

شماره	نام خانواده	مولفه امنیتی
الزام		
۶	مدیریت احراز هویت ناموفق (FIA_AFL)	**نام عنصر: ساماندهی شکست در احراز هویت ۱** **شماره مولفه: اش-ش‌ا.۱,۱.۱(FIA_AFL.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی، باید زمانی‌که به تعداد **یک عدد مثبت قابل تنظیم توسط سرپرست،** تلاش‌های ناموفق احراز هویت سرپرستی که از راه دور رخ می‌دهد را تشخیص دهند.
۷		**نام عنصر: ساماندهی شکست در احراز هویت ۱** **شماره مولفه: اش-ش‌ا.۱,۲(FIA_AFL.1.2)** **شرح مولفه:** زمانی‌که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید ، توابع امنیتی هدف ارزیابی باید

شماره	نام خانواده	مولفه امنیتی
		الزام

[انتخاب یکی از: از احراز هویت موفقیت آمیز سرپرست از راه دور جلوگیری کند تا زمانی‌که سرپرست محلی [اختصاص: اقدامی] را انجام دهد، از احراز هویت موفقیت آمیز سرپرست از راه دور جلوگیری کند تا زمانی‌که زمان تعریف شده توسط سرپرست سپری گردد] .

نکته کاربردی:

این الزام به سرپرست کنسول محلی اعمال نمی‌گردد، از این‌رو معنی ندارد که حساب کاربری سرپرست محلی در این مدل قفل گردد. این الزام می‌تواند (برای مثال) نیاز به یک حساب کاربری مجزا برای سرپرست محلی یا مجزا سازی سازوکارهای احراز هویت به صورت محلی و از راه دور اشاره کند. اقدام صورت گرفته توسط سرپرست محلی به طور خاص پیاده‌سازی می‌گردد و در سند راهنمای سرپرست تعریف می‌گردد (برای مثال، فعال‌سازی مجدد یا تنظیم مجدد رمز عبور). نویسنده هدف امنیتی، یکی از انتخاب‌های مطرح شده در بالا را انتخاب می‌نماید تا شکست‌های احراز هویت را مدیریت نماید با توجه به اینکه هدف ارزیابی چگونه این مدیریت را پیاده‌سازی می-نماید.

۸	خانواده گواهینامه-	**نام عنصر: گواهینامه‌های X509. ۱**

شماره	نام خانواده الزام	مولفه امنیتی
	های X509 (FIA-X509)	**شماره مولفه: اش-X509 (ت‌س).۱,۱(FIA-X509-EXT.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید از گواهینامه‌های x509v3 به صورت تعریف شده در RFC 5280 استفاده نمایند تا از احراز هویت برای IPsec و اتصالات [انتخاب: بدون پروتکل دیگر، TLS، SSH] پشتیبانی نمایند.
۹		**نام عنصر: گواهینامه‌های X509. ۱**
		شماره مولفه: اش-X509 (ت‌س).۲,۱(FIA-X509-EXT.1.2) **شرح مولفه:** توابع امنیتی هدف ارزیابی باید گواهینامه‌ها را برای جلوگیری از حذف و تغییر غیرمجاز، ذخیره و محافظت نمایند.
۱۰		**نام عنصر: گواهینامه‌های X509. ۱**

شماره	نام خانواده	مولفه امنیتی
الزام		

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

شرح مولفه:

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.

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

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

شرح مولفه:

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

نکته کاربردی:

شماره نام خانواده
مولفه امنیتی
الزام

کلید عمومی اشاره شده در مولفه «اش-.۴,۱X509»بخش کلید عمومی از جفت کلید خصوصی- عمومی تولید شده توسط هدف ارزیابی مشخص شده در «رز-م‌ک.۱(۲)» می‌باشد.

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

شماره مولفه: اش-X509 (ت‌س).۵,۱(FIA-X509-EXT.1.5)

شرح مولفه:

توابع امنیتی هدف ارزیابی باید گواهینامه‌ها را با استفاده از [انتخاب: پروتکل وضعیت گواهینامه‌های آنلاین به صورت مشخص شده در RFC 2560، لیست گواهینامه‌های باطل شده به صورت مشخص شده در] RFC 5759 اعتبارسنجی نمایند.

نکته کاربردی:

در حالیکه انتخاب روش ابطال به کار برده شده به نویسنده هدف امنیتی واگذار شده است، نسخه‌های آینده این بسته توسعه یافته الزام خواهد داشت که هر دو روش در دسترس سرپرست هدف ارزیابی باشد.

شماره	نام خانواده مولفه امنیتی الزام
۱۳	**نام عنصر: گواهینامه‌های X509. ۱** **شماره مولفه: اش-X509 (ت‌س).۱,۶(FIA-X509-EXT.1.6)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید مسیر گواهینامه بوسیله مطمئن شدن از وجود محدودیت‌های اصلی اضافه شده و True بودن پرچم CA برای تمام گواهینامه‌های CA، را اعتبارسنجی نمایند.
۱۴	**نام عنصر: گواهینامه‌های X509. ۱** **شماره مولفه: اش-X509 (ت‌س).۱,۷(FIA-X509-EXT.1.7)** **شرح مولفه:** در صورتیکه فیلد BasicConstraint در گواهینامه وجود نداشته باشد یا پرچم CA مقدار "true" نگرفته باشد، توابع امنیتی هدف ارزیابی نباید گواهینامه را به عنوان یک گواهینامه CA بکار ببرد.

شماره	نام خانواده مولفه امنیتی الزام
۱۵	**نام عنصر: گواهینامه‌های X509. ۱** **شماره مولفه: اش-X509 (ت‌س).۸,۱(FIA-X509-EXT.1.8)** **شرح مولفه:** توابع امنیتی هدف ارزیابی نباید یک SA[1]را برقرار نمایند اگر گواهینامه یا مسیر گواهینامه نامعتبر باشد.
۱۶	**نام عنصر: گواهینامه‌های X509. ۱** **شماره مولفه: اش-X509 (ت‌س).۹,۱(FIA-X509-EXT.1.9)** **شرح مولفه:** توابع امنیتی هدف ارزیابی نباید یک SA را برقرار نمایند، اگر نام مشخص[1] که در یک گواهینامه قرار گرفته است با نام مشخص مورد

1-Security Association

شماره نام خانواده
مولفه امنیتی
الزام

انتظار برای موجودیت‌هایی که در تلاش برای ایجاد یک اتصال هستند، منطبق نباشد.

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

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

شرح مولفه:

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

نکته کاربردی:

منظور از الزام«اش-X509-(ت‌س).۱۰,۱» آن است که چنان‌چه هدف ارزیابی نتواند به موجودیت مسئول ارائه‌ی اطلاعات اعتبارسنجی گواهینامه، متصل گردد، می‌تواند جهت اجازه برقراری نشست یا عدم اجازه برقراری نشست تنظیم گردد. برای مثال، اگر یک ارتباط با

1-Distinguished Name

شماره	نام خانواده	مولفه امنیتی
الزام		

CRL به علت خاموش بودن ماشین، یا قطع بودن مسیر شبکه ، برقرار نگردد، سرپرست می‌تواند هدف ارزیابی را به گونه‌ای تنظیم نماید که اجازه برقراری نشست را بدهد به جای آنکه از توانایی‌های هدف ارزیابی در ایجاد یک SA به علت در دسترس نبودن CA جلوگیری نماید.

۷,۴ کلاس مدیریت امنیت[1]

نام کلاس: مدیریت امنیت

شرح کلاس: این کلاس جهت مشخص نمودن 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 گردند.

این کلاس دارای چندین هدف است:

- مدیریت داده توابع امنیتی هدف ارزیابی برای مثال علامت‌ها[2]

[1]Security management (Class FMT)

[2]Banner

- 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 می-دهند.
- تعریف نقش‌های امنیتی

خانواده‌های آن در ادامه آمده است.

➢ خانواده مدیریت کارکرد توابع امنیتی هدف ارزیابی[1]

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 می‌باشد.

➢ خانواده مدیریت مشخصه‌های امنیتی[2]

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

[1]Management of functions in TSF (FMT_MOF)

[2]Management of security attributes (FMT_MSA)

امنیتی باشد.

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

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

- **خانواده لغو[2]**

این خانواده لغو مشخصه‌های امنیتی انواع موجودیت‌ها در هدف ارزیابی را آدرس‌دهی می‌کند.

- **خانواده انقضای مشخصه امنیتی[3]**

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

[1]Management of TSF data (FMT_MTD)

[2]Revocation (FMT_REV)

[3]Security attribute expiration (FMT_SAE)

➢ خانواده مشخصات کارکردهای مدیریت[1]

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 سرپرستان اجازه می‌دهند تا پارامترهایی برای کنترل عملکرد ویژگی‌های مربوط به امنیت هدف ارزیابی تعریف نماید، 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 می‌گردد تا تداوم عملکرد هدف ارزیابی را تضمین نماید، مانند عملکردهای پشتیبانی و بازیابی. عملکرد این خانواده بر روی دیگر مولفه‌ها 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	نام خانواده	مولفه امنیتی	الزام

[1]Specification of Management Functions (FMT_SMF)

[2]Security management roles (FMT_SMR)

شماره	نام خانواده	مولفه امنیتی
ه		
الزام		
۱۸	مشخصات کارکردهای مدیریت (FMT_SMF)	**نام عنصر:** مشخصات کارکردهای مدیریت ۱ **شماره مولفه: مد-ع‌م.۱،۱ (FMT_SMF.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید قادر به انجام کارکردهای مدیریت زیر باشند: • توانایی پیکربندی عملکرد رمزنگاری • توانایی پیکربندی عملکرد IPsec • توانایی سرپرست برای فعال نمودن، غیر فعال کردن و تعیین و تغییر رفتار تمام توابع امنیتی هدف ارزیابی که در این بسته توسعه یافته مشخص شده‌اند، • توانایی پیکربندی تمامی توابع مدیریت امنیتی که در دیگر بخش‌های این بسته توسعه یافته معرفی شده‌اند.

در این کلاس مدیریت امنیتی نسبت به NDPP الزامات بیشتری تعریف شده است، که در ادامه آورده شده است:

شماره	نام خانواده	مولفه امنیتی الزام
۱۹	مدیریت رفتار توابع امنیتی (FMT_MOF)	**نام عنصر:** مدیریت رفتار توابع امنیتی ۱ **شماره مولفه: م‌د-م‌ت.۱,۱ (FMT_MOF.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید قابلیت فعال‌سازی، غیر فعال‌سازی، تعیین و تغییر رفتار تمام توابع امنیتی هدف ارزیابی که در این بسته توسعه یافته معرفی شده است را به سرپرست احراز هویت شده محدود نمایند.

۷,۵ کلاس حفاظت از توابع امنیتی هدف ارزیابی[1]

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 می‌شوند و برای صحت و یکپارچگی داده توابع امنیتی هدف ارزیابی مورد استفاده قرار می‌گیرند. از بعضی جنبه‌ها، 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 سازوکاری مشابه 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 توابع امنیتی هدف ارزیابی نتوانند مورد مداخله قرار بگیرند یا دور زده[2]شوند.

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

- پیاده‌سازی توابع امنیتی هدف ارزیابی، که سازوکارهای اجرا کننده توابع امنیتی هدف ارزیابی را اجرا و پیاده‌سازی می‌نمایند.
- داده توابع امنیتی هدف ارزیابی، که پایگاه داده‌های سرپرستی، راهنمایی کننده اجرای الزامات کارکرد امنیتی می‌باشند.

[1]Protection of the TSF (Class FPT)

[2]Bypass

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

➢ خانواده نقض امنیت[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 می‌گردد.

➢ خانواده در دسترس بودن داده‌های ارسال شده توابع امنیتی هدف ارزیابی[2]

این خانواده قوانینی را تعریف می‌نماید 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 می‌نماید. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کُدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

➢ خانواده محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[3]

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

[1]Fail secure (FPT_FLS)

[2]Availability of exported TSF data (FPT_ITA)

[3]Confidentiality of exported TSF data (FPT_ITC)

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[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 می‌گردد. 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 می‌نماید که از داده توابع امنیتی هدف ارزیابی در زمان انتقال بین بخش‌های مجزای توابع امنیتی هدف ارزیابی در سراسر کانال داخلی محافظت می‌نماید.

- **خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[1]**

[1]Integrity of exported TSF data (FPT_ITI)

[2]Internal TOE TSF data transfer (FPT_ITT)

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

الزامات مولفه‌ها در این خانواده این اطمینان را می‌دهد که توابع امنیتی هدف ارزیابی از مداخله فیزیکی و تداخلات محافظت می‌گردد. ارضاء شدن این مولفه‌ها منجر به بسته‌بندی و استفاده توابع امنیتی هدف ارزیابی به صورتی گردد که مداخلات فیزیکی قابل تشخیص باشد یا مجبور به مقاومت در برابر تداخلات فیزیکی گردد. بدون این مولفه‌ها، عملکرد حفاظتی از توابع امنیتی هدف ارزیابی اثرشان را در محیط‌هایی که از آسیب فیزیکی نمی‌توان جلوگیری نمود، از دست می‌دهند این خانواده هم‌چنین الزاماتی را ارائه نموده است که چطور توابع امنیتی هدف ارزیابی باید به تلاش‌هایی که در ارتباط با تداخل فیزیکی صورت می‌گیرد واکنش نشان دهد.

- **خانواده بازیابی مطمئن[۲]**

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 می‌گردد و هم‌چنین می‌تواند بازیابی گردد. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی تعیین کننده حفاظت از وضعیت‌های بعدی می‌باشد.

- **خانواده شناسایی مجدد[۳]**

---

[1]TSF physical protection (FPT_PHP)

[2]Trusted recovery (FPT_RCV)

[3]Replay detection (FPT_RPL)

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

➢ خانواده پروتکل همگامی حالت[1]

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

در حالتی که عدم اعتماد به محیط توزیع وجود داشته باشد، به پروتکل همگام‌سازی پیچیده‌تری نیاز است.

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

➢ خانواده مهرهای زمانی[2]

این خانواده، الزاماتی را برای یک مهر زمانی معتبر در داخل هدف ارزیابی، آدرس‌دهی نموده است.

[1] State synchrony protocol (FPT_SSP)

[2] Time stamps (FPT_STM)

➢ خانواده سازگاری 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 اشتراک‌گذاری و تفسیر سازگار صفات و مجوزها، بین توابع امنیتی هدف ارزیابی مربوط به هدف ارزیابی و یک محصول امن IT متفاوت تعریف می-نماید.

➢ خانواده آزمون موجودیت‌های خارجی[2]

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف می‌نماید تا تست‌هایی را بر روی یک با بیش از یک موجودیت خارجی انجام دهد. عناصر مطرح شده در این خانواده برای اعمال به کاربران انسانی در نظر گرفته نشده‌اند.

موجودیت‌های خارجی، ممکن است شامل برنامه‌هایی باشد که بر روی هدف ارزیابی اجرا می‌گردند، سخت‌افزار و نرم‌افزاری که تحت هدف ارزیابی اجرا می-گردند (پلتفرم‌ها، سیستم‌عامل و ...) یا برنامه‌ها و باکس‌های متصل شده به هدف ارزیابی (سیستم‌های تشخیص نفوذ، فایروال‌ها، سرورهای ورود، سرورهای زمانی و غیره) باشد.

➢ خانواده سازگاری در تکرار داده‌ها در توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی[3]

---

[1]Inter-TSF TSF data consistency (FPT_TDC)

[2]Testing of external entities (FPT_TEE)

[3]Internal TOE TSF data replication consistency (FPT_TRC)

الزامات این خانواده از آن جهت لازم و ضروری می‌باشد، تا از سازگاری داده توابع امنیتی هدف ارزیابی زمانی‌که در داخل هدف ارزیابی تکرار می‌گردد، اطمینان حاصل نماید. منظور از سازگاری داده‌ها، یکسان بودن داده‌ها در محل‌ها و توابع مختلف است. داده توابع امنیتی هدف ارزیابی زمانی ناسازگار می‌شود که کانال داخلی بین بخش‌های مختلف هدف ارزیابی نامعتبر گردد. اگر اجزای هدف ارزیابی از نظر داخلی تشکیل یک شبکه دهند، در صورت غیر فعال شدن ارتباطات شبکه‌ای، عدم سازگاری بین داده‌های 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 می‌نماید. اجبار هدف ارزیابی به انجام تست بر روی بخش‌های حساس و مهم هدف ارزیابی با استفاده از نمونه عملیات‌های ریاضی مثالی از این الزام می‌باشد. این‌گونه تست‌ها 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 می‌گردد.

الزامات این خانواده هم‌چنین برای تشخیص عدم صحت داده توابع امنیتی هدف ارزیابی و یا خود توابع امنیتی هدف ارزیابی (کد اجرایی یا مولفه‌های 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 می‌توانند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط در طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهند یا به دلیل تغییر مخرب توابع امنیتی هدف ارزیابی بر اثر حفاظت منطقی و/یا فیزیکی ناکافی صورت بگیرند.

[1] TSF self test (FPT_TST)

شماره	نام خانواده	مولفه امنیتی
الزام		
۲۰	به روز رسانی امن (FPT_TUD_EXT)	**نام عنصر:** به روز رسانی امن ۱ **شماره مولفه: حت-رم-(ت‌س).۳,۱ (FPT_TUD_EXT.1.3)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید این قابلیت را داشته باشد تا به روزرسانی‌های نرم‌افزار/میان‌افزار هدف ارزیابی را با استفاده از سازوکار امضای دیجیتال و [انتخاب: درهم‌سازی منتشر شده، هیچ عملکرد دیگر] بررسی نماید، پیش از آنکه به روزرسانی‌ها نصب گردد. **نکته کاربردی:** NDPP این امکان را فراهم کرده است که روش تائید به روزرسانی را نویسنده هدف امنیتی در صورت تمایل مشخص نماید. برای مطابقت با این بسته توسعه یافته، سازوکار امضای دیجیتال (یکی از سازوکارهایی که در رز-ع‌ر.۱ (۲) مشخص شده است) باید به کار رود.
۲۱	خودآزمایی توابع امنیتی هدف ارزیابی (FPT_TST)	**نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی۱** **شماره مولفه: حت-خا-(ت‌س).۲,۱ (FPT_TST_EXT.1.2)**

شماره نام خانواده
الزام **مولفه امنیتی**

شرح مولفه:

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 راستی آزمایی گردند.

نکته کاربردی:

NDPP برای این عنصر شامل یک مولفه است، که ملزم می‌نماید یک مجموعه خودآزمایی‌های نشان دهنده عملکرد صحیح توابع امنیتی هدف ارزیابی می‌باشد. این مولفه به عنصر مطابق این بسته توسعه یافته اضافه می‌شود.

در کلاس حفاظت از توابع ارزیابی، نسبت به NDPP الزامات بیشتری تعریف شده است که در ادامه آمده است:

شماره الزام	نام خانواده مولفه امنیتی	
۲۲	**نام عنصر:** نقض امنیت ۱ **شماره مولفه: حت-ن‌ا.۱,۱ (FPT_FLS.1.1)** **شرح مولفه:** توابع امنیتی هدف ارزیابی باید زمانی‌که انواع شکست‌های زیر رخ می‌دهد، از کار انداخته شود: • شکست خودآزمایی‌های روشن کردن • شکست بررسی یکپارچگی image قابل اجرای توابع امنیتی هدف ارزیابی • شکست آزمون‌های سالم بودن منابع نویز **نکته کاربردی:** شکست‌های مربوط به این الزام، الزام حت-خا-(ت‌س).۱,۱ در NDPP و الزام حت-خا-(ت‌س).۲,۱مشخص شده در این بسته توسعه یافته	نقض امنیت (FPT_FLS)

شماره	نام خانواده	مولفه امنیتی	الزام
			هستند.

۷,۶ کلاس فیلتر نمودن بسته‌ها

شماره	نام خانواده	مولفه امنیتی	الزام
۲۳	**نام عنصر: فیلترنمودن بسته‌ها۱** **شماره مولفه: ف‌ب-ق‌ن-(ت‌س).۱,۱ (FPF_RUL_EXT.1.1)** **شرح مولفه:**	فیلترنمودن بسته‌ها (FPF_RUL_EXT)	توابع امنیتی هدف ارزیابی، باید برروی بسته‌های شبکه‌ای که توسط هدف ارزیابی پردازش می‌شود، فیلترنمودن ترافیک را انجام دهد.
۲۴	**نام عنصر: فیلترنمودن بسته‌ها ۱**		

شماره نام خانواده

الزام

مولفه امنیتی

شماره مولفه: ف‌ب-ق‌ن-(ت‌س).۲,۱.۱ (FPF_RUL_EXT.1.2)

شرح مولفه:

توابع امنیتی هدف ارزیابی، باید پروتکل‌های ترافیک شبکه زیر را پردازش نماید:

- پروتکل اینترنت (IPv4)
- پروتکل اینترنت نسخه۶ (IPv6)
- پروتکل کنترل انتقال (TCP)
- پروتکل دیتاگرام داده (UDP)

و تا حدی که در دیگر مولفه‌های این الزام امنیتی ضروری است، قادر به بررسی فیلد سرآیند بسته‌های شبکه که در RFC های زیر تعریف شده‌اند، باشد:

- RFC 791(IPv4)

شماره نام خانواده

مولفه امنیتی

الزام

- RFC 2460(IPv6)
- RFC 793(TCP)
- RFC 768 (UDP)

نکته کاربردی:

این مولفه[1]مشخص کننده پروتکل‌ها و مراجع تعریف پروتکل است که مورد استفاده قرار می‌گیرند تا تعریف کنند که چه حدی از ترافیک شبکه توسط هدف ارزیابی در زمان ورود (دریافت ترافیک شبکه یا ورود[2]) و خروج (فرستادن ترافیک شبکه یا خروج) مورد تفسیر و بررسی قرار گیرد.

از آنجا که قالب پروتکل‌های مشخص شده در RFCها هنوز مورد استفاده قرار می‌گیرند، بسیاری از RFCها رفتارهایی را تعریف می‌نمایند که امروزه ثابت شده است که امن نیستند. به عنوان نمونه در RFC شماره ۷۹۲ نوع بسته کنترلی به نام "redirect" تعریف شده است که

[1]Element

[2]Ingress

شماره	نام خانواده	مولفه امنیتی	الزام
		امن نمی باشد.	
۲۵		**نام عنصر: فیلترنمودن بسته‌ها ۱**	
		شماره مولفه: ف‌ب-ق‌ن-(ت‌س).۳,۱.۱ (FPF_RUL_EXT.1.3)	
		شرح مولفه:	
		توابع امنیتی هدف ارزیابی، باید قوانین فیلترنمودن ترافیک را با استفاده از فیلدهای پروتکل شبکه زیر و واسطهای مجزا تعریف نماید:	
		• IPv4	
		- آدرس مبدا	
		- آدرس مقصد	
		- پروتکل	
		• IPv6	

شماره نام خانواده

الزام **مولفه امنیتی**

- آدرس مبدا

- آدرس مقصد

- سرآیند[1] بعدی (پروتکل)

- TCP

- پورت مبدا

- پورت مقصد

- UDP

- پورت مبدا

- پورت مقصد

[1] Header

شماره	نام خانواده	مولفه امنیتی
الزام		

نکته کاربردی:

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

هم‌چنین «واسط» که در بالا معرفی شده است پورت خروجی است که ترافیک شبکه اجرایی را دریافت و یا به طور متناوب ارسال خواهد نمود.

۲۶ **نام عنصر: فیلترنمودن بسته‌ها ۱**

شماره مولفه: ف‌ب-ق‌ن-(ت‌س).۴,۱.۱ (FPF_RUL_EXT.1.4)

شرح مولفه:

توابع امنیتی هدف ارزیابی، باید امکان انجام عملکردهای زیر را برای هر یک از قوانین فیلتر نمودن حالتمند شبکه فراهم آورد:

- اجازه داده

شماره نام خانواده

مولفه امنیتی

الزام

- جلوگیری کردن
- گزارش‌گیری

نکته کاربردی:

این عنصر، عملکردهایی را تعریف می‌نماید که می‌تواند با قوانینی استفاده شده مطابق با ترافیک شبکه مرتبط گردد. قابل ذکر است که داده‌های گزارش‌گیری شده در الزام ممیزی امنیت معرفی شده‌اند.

۲۷ **نام عنصر: فیلترنمودن بسته‌ها ۱**

شماره مولفه: ف‌ب-ق‌ن-(ت‌س).۵,۱.(FPF_RUL_EXT.1.5)

شرح مولفه:

توابع امنیتی هدف ارزیابی، باید امکان اعمال هر یک از قوانین فیلتر نمودن حالتمند شبکه را بر روی هر یک از واسطهای شبکه فراهم آورد.

شماره	نام خانواده	مولفه امنیتی
الزام		

نکته کاربردی:

این عنصر محل اعمال قوانین را مشخص می‌کند. یک هدف ارزیابی مطابق با این پروفایل حفاظتی، باید قادر باشد که قوانین فیلتر نمودن را به هریک از واسط‌های شبکه که در دسترس هستند و قابل مشخص شدن باشند و ترافیک شبکه لایه ۳و ۴ را به کار می‌برند، اعمال نماید. قابل شناسایی به این معنی است که واسط‌ها در داخل هدف ارزیابی منحصربه فرد و قابل شناسایی است، و لزوماً به واسطی که از دید شبکه قابل مشاهده باشد، اشاره ندارد (به طور مثال لازم نیست که حتما به آن واسط آدرس اینترنتی اختصاص داده شده باشد).

قابل ذکر است که می‌توان یک مجموعه قوانین مجزا برای هر واسط داشته باشد یا یک مجموعه قوانین مشترک برای واسط‌های مشخصی اعمال شود.

۲۸ **نام عنصر: فیلترنمودن بسته‌ها ۱**

شماره مولفه: ف‌ب-ق‌ن-(ت‌س).۶,۱.۱ (FPF_RUL_EXT.1.6)

شماره نام خانواده

مولفه امنیتی

الزام

شرح مولفه:

توابع امنیتی هدف ارزیابی باید قوانین اجرایی فیلترنمودن ترافیک را به ترتیب زیر پردازش نماید (به‌صورتیکه در ف‌و‌-ف‌ت.(ت‌س).۱,۵.مشخص شده است):

- تعریف شده توسط سرپرست

نکته کاربردی:

این عنصر لازم و ضروری است تا سرپرست قادر به تعریف نمودن ترتیب اعمال قوانین فیلترنمودن باشد.

۲۹ **نام عنصر: فیلترنمودن بسته‌ها ۱**

شماره مولفه: ف‌ب‌-ق‌ن‌-(ت‌س).۷,۱.۱ (FPF_RUL_EXT.1.7)

شرح مولفه:

شماره	نام خانواده	مولفه امنیتی
الزام		

توابع امنیتی هدف ارزیابی باید از عبور بسته‌ها جلوگیری نمایند، در صورتی‌که هیچ قانون تطابقی تعریف نشده باشد.

نکته کاربردی:

این عنصر الزام می‌دارد که بجز زمانی‌که یک بسته جزئی از یک ارتباط شروع شده باشد، در زمانی‌که هیچ قاونی اعمال نگردد، رفتار هدف ارزیابی در حالت کلی بر جلوگیری از عبور بسته‌ها باشد.

۷,۷ کلاس کانال‌ها و مسیرهای مورد اعتماد[1]

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

نام کلاس: کانال‌ها / مسیرهای مورد اعتماد

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

[1]Trusted path/channels(Class FTP)

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 دستورها را از باقی توابع امنیتی هدف ارزیابی و داده کاربر جداسازی می‌نماید.
- استفاده از مسیر ارتباطی ممکن، توسط کاربر یا توابع امنیتی هدف ارزیابی آغاز گردد.
- 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 گردد و ارائه دهنده شاخصه 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 اغلب 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 گردد. پاسخ امن از طریق مسیر امن تضمین می‌کند که از تغییرات توسط برنامه ناامن یا افشا شدن برای یک برنامه ناامن محافظت می‌نماید.

➢ کانال مورد اعتماد 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

[1]Inter-TSF trusted channel(FTP_ITC)

محصولات امن IT وجود دارد، در نظر گرفته شود.

➢ مسیر مورد اعتماد[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 گردد، یا توابع امنیتی هدف ارزیابی ممکن است از طریق مسیر امن، ارتباطی را با کاربر برقرار نمایند.

شماره الزام	نام خانواده	مولفه امنیتی
۳۰	کانال مورد اعتماد بین توابع امنیتی هدف ارزیابی مم-کم **(FTP_ITC)**	**نام عنصر: کانال مورد اعتماد بین توابع امنیتی هدف ارزیابی ۱** **شماره مولفه: مم-کم.۱,۱ (FTP_ITC.1.1)** **شرح مولفه:**

[1]Trusted path(FTP_TRP)

شماره نام خانواده

مولفه امنیتی

الزام

توابع امنیتی هدف ارزیابی باید از پروتکل IPsec و [انتخاب: SSH، TLS،TLS/HTTPS ، هیچ پروتکل دیگر] استفاده نمایند تا یک کانال ارتباطی امن بین خود و تمام موجودیت‌های IT مجاز ایجاد نمایند، به طوریکه این کانال بصورت منطقی از دیگر کانال‌های ارتباطی مجزا بوده و نقطه پایانی ارتباط را به طور قطعی شناسایی نماید و از داده کانال در برابر افشا و تشخیص تغییرات داده کانال محافظت نماید.

نکته کاربردی:

NDPP به کانال‌های امن دیگری به غیر از IPsec نیز اجازه می‌دهد تا برای ارتباط با موجودیت IT خارجی مورد استفاده قرار بگیرند. برای مطابقت با این بسته توسعه یافته، انتخاب باید به گونه‌ای باشد که هدف ارزیابی پروتکل IPsec را به عنوان یک گزینه قابل تنظیم به سرپرست ارائه دهد.