به نام خدا

پروفایل حفاظتی هانی پات تعامل کم

اردیبهشت ۱۳۹۴

نسخه ۱,۰

با تشکر و سپاس از نظرات و پیشنهادات

شرکت صبا سیستم صدرا
مرکز تحقیقات صنایع انفورماتیک

فهرست

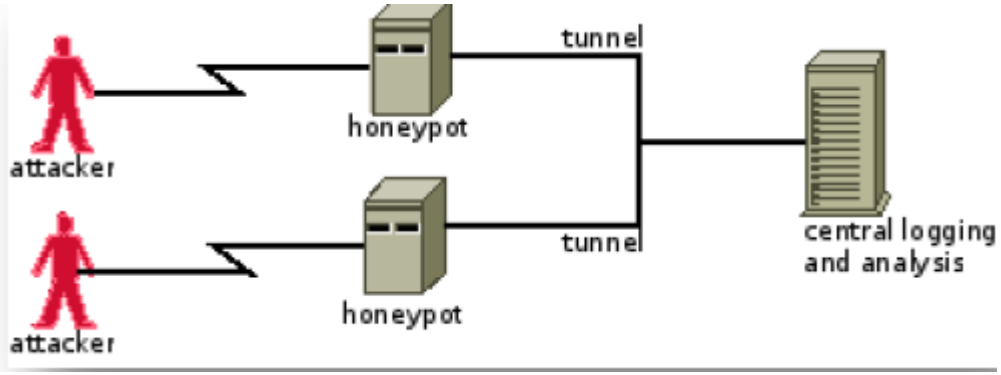
۱مقدمه

این سند که در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است، برای بیان الزامات کارکرد امنیتی هر محصول لازم است. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات ارائه شده‌اند، در محصول خود فراهم و به خریداران آن محصول نیز در انتخاب محصول خود کمک کنند.. این سند به الزامات امنیتی هانی پات‌های با تعامل کم می‌پردازد.

این سند بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408تهیه گردیده است. همچنین فرهنگ اصطلاحات بکار رفته در این سند در پیوست شماره یک آمده است.

۲ شرح محصول

این پروفایل حفاظتی، حداقل الزامات امنیتی برای هدف ارزیابی (مدیریت متمرکز هانی پات‌های با تعامل کم) مشخص می‌نماید. سیستم از یک یا بیش از یک حس‌گر (هانی پات‌های خاص منظور) که می‌تواند به‌صورت مجزا یا به‌صورت یکپارچه تجهیز شده باشند به همراه یک سیستم مدیریت متمرکز تشکیل‌شده‌اند. حس‌گرها با استفاده از یک سیستم مدیریت متمرکز پیکره‌بندی و مدیریت می‌شوند؛ و هر یک از این حس‌گرها مشاهدات و اطلاعات خود را به سیستم مرکزی ارسال می‌کنند.



شکل ۱: هانی پات‌ها و سیستم مدیریت متمرکز در شبکه

هانی پات‌ها یک فنّاوری اطلاعاتی است که ارزش آن به استفاده غیرمجاز و ممنوع دیگران از آن است و تمامی هانی پات‌ها بر اساس این ایده کار می‌کنند که: هیچ‌کس نباید از آن‌ها استفاده کند و یا با آن‌ها تعامل برقرار نماید، هر تعاملی با هانی پات‌ها غیرمجاز شمرده‌شده و نشانه‌ای از یک حرکت خرابکارانه به شمار می‌رود. یک هانی پات سامانه‌ای است که در شبکه سازمان قرار می‌گیرد، اما برای کاربران آن شبکه کاربردی ندارد و در حقیقت هیچ‌یک از افراد سازمان حق برقراری ارتباط با آن را ندارند. این سیستم دارای یک سری ضعف‌های امنیتی عمدی است. ازآنجایی‌که مهاجمان برای نفوذ به یک شبکه همیشه به دنبال سامانه‌های دارای ضعف می‌گردند، این سیستم توجه آن‌ها را به خود جلب می‌کند و با توجه به اینکه هیچ‌کس حق ارتباط با این سیستم را ندارد، پس هر تلاشی برای برقراری ارتباط با این سیستم، یک تلاش خرابکارانه از سوی مهاجمان محسوب می‌شود. در حقیقت این سیستم نوعی دام است که مهاجمان را فریب داده و به‌سوی خود جلب می‌کند و به‌این‌ترتیب علاوه بر امکان نظارت و کنترل کار مهاجمان، این فرصت را نیز به سازمان می‌دهد که فرد مهاجم را شناسایی کند و از سامانه‌های اصلی شبکه خود دورنگه دارند.

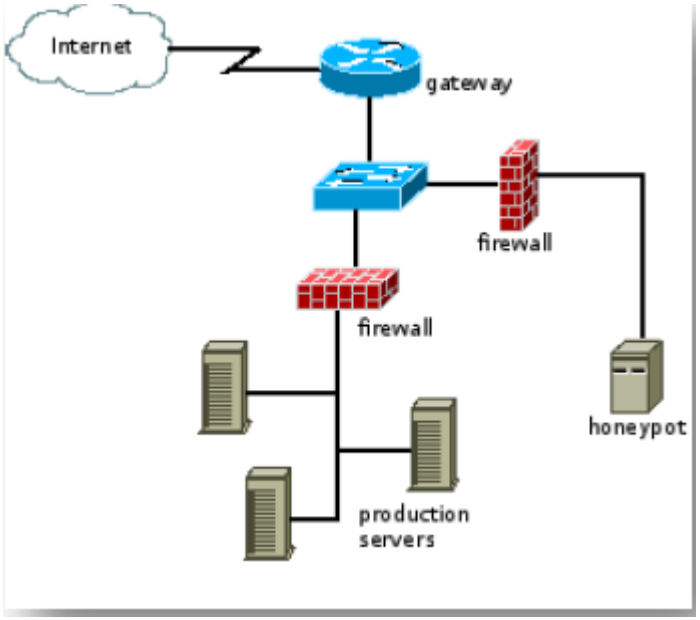
هانی پات‌ها را می‌توانیم به دو گروه، با تعامل کم[1] و با تعامل زیاد[2] تقسیم کنیم. منظور از تعامل، میزان فعالیت است که یک فرد مهاجم اجازه دارد با آن هانی پات انجام دهد . هر چه این میزان فعالیت و تعامل بیشتر باشد، فرد مهاجم کارهای بیشتری می‌تواند انجام دهد و در نتیجه می‌توان راجع به وی و فعالیتش اطلاعات بیشتری به دست آورد. البته با افزایش این فعالیت و تعامل، میزان ریسک نیز افزایش می‌یابد. هانی پات های با تعامل کم اجازه انجام حجم کمی از تعاملات را صادر می‌کنند، درحالی‌که هانی پات های با تعامل زیاد حجم زیادی از تعاملات را اجازه می‌دهند.

در این پروفایل حفاظتی منظور از هانی پات در واقع هانی پات‌های با تعامل کم (حس‌گر) است که با شبیه‌سازی سامانه‌ها و سرویس‌ها کار می‌کنند و فعالیت‌های مهاجمان نیز صرفاً شامل همان مواردی است که سرویس‌های شبیه‌سازی‌شده اجازه می‌دهند.

هانی پات‌ها در شبکه برای دو هدف مهاجمان داخلی و مهاجمان خارجی به کار گرفته می‌شود. رایج‌ترین استقرار برای هانی پات، پیکره‌بندی آن‌ها برای اهداف اینترنتی است. که در این مورد هانی پات در DMZ قرار می‌گیرد. شکل ۲ نمای این استقرار را نمایش می‌دهد.

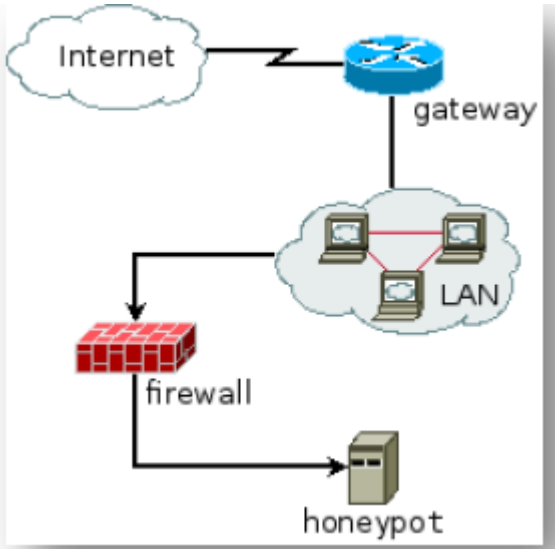
[1] Low Interaction

[2] High interaction



شکل ۲: استقرار هانی پات در DMZ

شیوه دوم استقرار برای تشخیص نفوذ مهاجمان درون شبکه است که شکل زیر نحوه استقرار هانی پات و دیگر اجزای شبکه را نشان می‌دهد. در این نوع استقرار هانی پات باید در سگمنت LAN قرارگرفته و به آن آدرس‌های IP بدون استفاده را تخصیص داد.



شکل ۳: استقرار هانی پات در سگمنت LAN

۳ تعریف مسائل امنیتی

۳,۱ فرضیات

A.TYPE	توضیحات
A.ACCESS	هدف ارزیابی به تمام داده‌های سیستم IT که در اجرای عملکردش به آن‌ها نیاز دارد، دسترسی دارد.
A.DYNMIC	هدف ارزیابی به صورتی مدیریت خواهد شد تا به‌صورت مناسبی تغییرات در سیستم IT که هدف ارزیابی مانیتور می‌نماید را آدرس‌دهی نماید.

A.ASCOPE	هدف ارزیابی به‌صورت مناسبی به سیستم IT که هدف ارزیابی مانیتور می‌نماید، قابل تنظیم[1] است.
A.PROTCT	سخت‌افزار و نرم‌افزار هدف ارزیابی که به اجرای سیاست‌های امنیتی حساس هستند از تغییرات فیزیکی غیرمجاز، محافظت می‌گردند.
A.LOCATE	منابع پردازشی هدف ارزیابی در جاهایی قرار می‌گیرند که دسترسی کنترل‌شده‌ای داشته باشند، تا از دسترسی فیزیکی غیرمجاز جلوگیری گردد.
A.MANAGE	یک یا بیش از یک کامپوننت مجزا وجود خواهد داشت که اختصاص به مدیریت هدف ارزیابی و امنیت اطلاعات آن دارد.
A.NOEVIL	سرپرستان مجاز افراد بی‌دقت، عمداً مسامحه‌کار یا متخاصم نیستند، و دستورالعمل‌های ارائه‌شده در مستندات راهنما را دنبال می‌نمایند.
A.NOTRST	هدف ارزیابی تنها توسط کاربران مجاز می‌تواند دستیابی گردد.

۳,۲ تهدیدات

T.TYPE	توضیحات
T.COMINT	یک کاربر غیرمجاز ممکن است سعی نماید تا با دور زدن سازوکارهای امنیتی، صحت داده‌های جمع‌آوری‌شده و تولیدشده توسط هدف ارزیابی را به خطر اندازد.
T.COMDIS	یک کاربر غیرمجاز ممکن است سعی نماید تا با دور زدن سازوکارهای امنیتی، داده‌های جمع‌آوری‌شده و تولیدشده توسط هدف ارزیابی را افشاء نماید.
T.LOSSOF	یک کاربر غیرمجاز ممکن است سعی نماید تا داده‌های جمع‌آوری‌شده و تولیدشده توسط هدف ارزیابی را از بین ببرد یا منتقل نماید.

[1] Scalable

T.NOHALT	یک کاربر غیرمجاز ممکن است سعی نماید تا با متوقف نمودن اجرای هدف ارزیابی، استمرار جمع‌آوری‌کننده سیستم و عملکرد تحلیل را به خطر اندازد.
T.PRIVIL	یک کاربر غیرمجاز ممکن است دستیابی به سیستم را به دست آورد و با استخراج نمودن مجوزهای سیستم به داده و عملکرد امنیتی هدف ارزیابی، دستیابی پیدا نماید.
T.IMPCON	یک کاربر غیرمجاز ممکن است با تغییر دادن پیکربندی هدف ارزیابی سبب گردد نفوذهای بالقوه، تشخیص داده نشوند.
T.INFLUX	یک کاربر غیرمجاز ممکن است با نفوذ دادن داده‌هایی که هدف ارزیابی نمی‌تواند به کار ببرد[۱]، سبب سوء عمل هدف ارزیابی گردد.
T.FACCNT	تلاش‌های غیرمجاز جهت دستیابی به داده هدف ارزیابی یا عملکرد امنیتی، ممکن است تشخیص داده نشود.
T.SCNCFG	ممکن است در سیستم IT که هدف ارزیابی آن را مانیتور می‌نماید، تنظیمات پیکربندی امنیتی نامناسبی وجود داشته باشد.
T.SCNMLC	کاربران می‌توانند با اجرای کدهای مخرب بر روی سیستم IT که هدف ارزیابی مانیتور می‌نماید، سبب تغییرات داده‌های محافظت‌شده سیستم IT یا تحلیل عملکرد امنیتی سیستم IT گردند.
T.SCNVUL	ممکن است در سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، آسیب‌پذیری‌هایی وجود داشته باشد.
T.FALACT	واکنش هدف ارزیابی به آسیب‌پذیری‌های شناسایی‌شده یا مورد ظن یا فعالیت‌های نامناسب، ممکن است با شکست مواجه گردد.
T.FALASC	هدف ارزیابی ممکن است در شناسایی آسیب‌پذیری‌ها یا فعالیت‌های نامناسب بر اساس تمام داده‌های سیستم تشخیص نفوذ[۲]که از تمام منابع داده دریافت شده است، با شکست مواجه گردد.
T.MISUSE	دستیابی‌ها و فعالیت‌های غیرمجاز ممکن است ناشی از بد به کار بردن سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، باشد.

[۱] Handle

[۲] Intrusion Detection System

T.INADVE	دستیابی‌ها و فعالیت‌های غیرعمدی ممکن است بر روی سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، رخ دهد.
T.MISACT	فعالیت‌های مخربی، همچون منتشر نمودن اسب‌های تروجان و ویروس‌ها، ممکن است بر روی سیستم IT که توسط هدف ارزیابی مانیتور می‌گردد، رخ دهد.

۳,۳ خط‌مشی‌ها

P.TYPE	توضیحات
P.DETECT	اطلاعات پیکربندی ایستا که ممکن است نشان‌دهنده پتانسیلی برای نفوذ بعدی یا وقوع نفوذ قبلی سیستم IT باشد یا رویدادهایی که نشان‌دهنده فعالیت‌های نامناسب است که منجر به بد به کاربردن، دستیابی و فعالیت‌های مخربی از دارایی‌های سیستم IT می‌شوند، باید جمع‌آوری گردند.
P.MANAGE	هدف ارزیابی باید به‌تنهایی توسط کاربران مجاز مدیریت گردد.
P.ACCESS	تمام داده‌های جمع‌آوری‌شده و تولیدشده توسط هدف ارزیابی باید تنها برای اهداف مجاز استفاده گردند.
P.ACCACT	کاربران هدف ارزیابی باید پاسخگوی اقداماتشان در داخل سیستم تشخیص نفوذ باشند.
P.INTGTY	داده‌های جمع‌آوری‌شده و تولیدشده توسط هدف ارزیابی باید از تغییرات حفظ گردند.
P. PROTCT	هدف ارزیابی باید از دستیابی غیرمجاز و قطع شدن داده‌های هدف ارزیابی و عملکردشان محافظت نماید.

۴ اهداف امنیتی

۴,۱ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.PROTCT	هدف ارزیابی باید خود را از تغییرات غیرمجاز و دستیابی به عملکرد و داده‌اش حفظ نماید.
O.HONEYPOTCAN	اسکنر باید اطلاعات پیکربندی ایستا را که ممکن است حاکی از پتانسیلی برای نفوذ بعدی یا وقوع نفوذ قبلی از یک سیستم

	IT باشند را جمع‌آوری و ذخیره نماید.
O.HONEYPOTENS	حس‌گرها باید اطلاعات مرتبط با تمام رویدادهایی که نشان‌دهنده فعالیت نامناسبی هستند را جمع‌آوری و ذخیره نمایند این فعالیت‌ها ممکن است منجر به بد به کار بردن، دستیابی یا فعالیت‌های مخربی در رابطه با دارایی‌های سیستم IT و سیستم تشخیص نفوذ گردند.
O.RESPON	هدف ارزیابی باید به نتایج تحلیلی پاسخ مناسبی بدهند.
O.EADMIN	هدف ارزیابی باید دارای عملکردهایی باشد که بتواند به‌صورت مؤثر عملکردها و داده‌هایش را مدیریت نماید.
O.ACCESS	هدف ارزیابی باید اجازه بدهد که کاربران مجاز تنها به عملکردها و داده‌های مناسب هدف ارزیابی دسترسی داشته باشند.
O.IDAUTH	هدف ارزیابی پیش از آنکه به کاربران اجازه دستیابی به عملکردها و داده‌های هدف ارزیابی را بدهد، باید قادر به شناسایی و احراز هویت آن‌ها باشد.
O.OFLOWS	هدف ارزیابی باید به‌صورت مناسبی سرریز ذخیره داده سامانه‌ای و ممیزی را مدیریت نماید.
O.AUDITS	هدف ارزیابی باید رکوردهای ممیزی را برای دستیابی داده و استفاده از عملکرد سیستم ثبت نماید.
O.INTEGR	هدف ارزیابی باید نسبت به صحت تمام داده‌های ممیزی و سامانه‌ای اطمینان حاصل نماید.
O.EXPORT	زمانی که هر کامپوننت سیستم هانی پات سبب گردد داده‌اش در دسترس کامپوننت سیستم هانی پات دیگری قرار گیرد، هدف ارزیابی اطمینان خواهد داد که داده سامانه‌ای محرمانه است.

۴,۲ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.AUDIT_PROTECTION	محیط IT قابلیت محافظت از اطلاعات ممیزی را فراهم خواهد نمود.
OE.AUDIT_SORT	محیط IT قابلیت مرتب‌سازی اطلاعات ممیزی را فراهم خواهد نمود.

OE.TIME	محیط IT قابلیت مهرهای زمانی قابل‌اطمینانی را به هدف ارزیابی ارائه خواهد نمود.
OE.INSTAL	کسانی که مسئول هدف ارزیابی هستند باید اطمینان بدهند که هدف ارزیابی به صورتی دریافت، نصب، مدیریت‌شده و هم-چنین عمل می‌نماید که با امنیت IT سازگار باشد.
OE. PHISYCAL	کسانی که مسئول هدف ارزیابی هستند باید اطمینان بدهند که بخش‌هایی از هدف ارزیابی که به سیاست امنیتی حساس هستند از هرگونه حمله فیزیکی محافظت می‌گردند
OE.CREDEN	کسانی که مسئول هدف ارزیابی هستند باید اطمینان بدهند که تمام گواهینامه‌های دستیابی توسط کاربران به صورتی محافظت می‌گردد که با امنیت IT سازگار باشد.
OE.PERSON	افرادی که به عنوان سرپرستان مجاز فعالیت می‌نمایند باید با دقت انتخاب شوند و از قبل آموزش ببینند.
OE.INTROP	هدف ارزیابی با سیستم IT که مانیتور می‌گردد، قابل تفسیر [۱]است.

۵ الزامات کارکرد امنیتی هانی پات با تعامل کم

کلاس‌های کارکرد امنیتی	الزام	نام الزام	رخدادهای قابل ممیزی	الزامات
کلاس ممیزی امنیت (FAU)	FAU_GEN.1	تولید داده ممیزی	هیچ	
	FAU_GEN.2	مرتبط نمودن هویت کاربر به رخداد	هیچ	
	FAU_STG_EXT.1	ذخیره‌سازی رخدادهای ممیزی	هیچ	

[۱] Interoperable

		امنیت		
کلاس پشتیبانی از رمزنگاری (FCS)	FCS_CKM.1	مدیریت کلید رمزنگاری	هیچ	
	FCS_CKM_EXT.4	مدیریت کلید رمزنگاری	هیچ	
	FCS_COP.1(1)	عملیات رمزنگاری	هیچ	
	FCS_COP.1(2)	عملیات رمزنگاری	هیچ	
	FCS_COP.1(4)	عملیات رمزنگاری	هیچ	
	FCS_RBG_EXT.1	تولید بیت تصادفی	هیچ	
کلاس حفاظت از داده‌های کاربری (FDP)	FDP_RIP.2	حفاظت از داده‌های باقی‌مانده	هیچ	
کلاس شناسایی و احراز هویت (FIA)	FIA_PMG_EXT.1	مدیریت رمز عبور	هیچ	
	FIA_UIA_EXT.1	شناسایی و احراز هویت کاربر	همه مواردی که از سازوکار شناسایی و احراز هویت استفاده می‌نمایند.	ارائه کردن شناسه کاربری، مبدأ تلاش(به‌طور مثال IP address)
	FIA_UAU_EXT.2	شناسایی و احراز هویت کاربر	همه مواردی که از سازوکارهای احراز هویت استفاده می‌نمایند.	مبدأ تلاش(به‌طور مثال IP address)
کلاس مدیریت (FMT)	FMT_MTD.1	مدیریت داده‌های توابع امنیتی هدف ارزیابی	هیچ	
	FMT_SMF.1	مشخصات کارکردهای مدیریتی	هیچ	
	FMT_SMR.2	محدودسازی نقش‌های امنیتی	هیچ	

کلاس حفاظت از توابع هدف ارزیابی(FPT)	FPT_SKP_EXT.1	محافظت از داده‌های توابع امنیتی هدف ارزیابی	هیچ	
	FPT_APW_EXT.1	حفاظت از کلمه عبور سرپرست	هیچ	
	FPT_STM.1	مهرهای زمانی	تغییرات زمانی	مقادیر جدید و قدیم برای زمان مبدأ تلاش (به‌طور مثال IP address)
	FPT_TUD_EXT.1	به‌روزرسانی امن	شروع به‌روزرسانی	بدون هیچ اطلاعات اضافه
	FPT_TST_EXT.1	محافظت از داده‌های توابع امنیتی هدف ارزیابی	هیچ	
کلاس دسترسی هدف ارزیابی(FTA)	FTA_SSL_EXT.1	قفل‌گذاری بر روی نشست‌ها و خاتمه دادن به آن‌ها	هرگونه تلاش در بازنمودن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
	FTA_SSL.3	قفل‌گذاری بر روی نشست‌ها و خاتمه دادن به آن‌ها	پایان دادن از راه دور نشست توسط سازوکارهای قفل نمودن نشست	بدون هیچ اطلاعات اضافه
	FTA_SSL.4	قفل‌گذاری بر روی نشست‌ها و خاتمه دادن به آن‌ها	پایان دادن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
	FTA_TAB.1	علائم دسترسی هدف ارزیابی	هیچ	
کلاس مسیر امن(FTP)	FTP_ITC.1	کانال مورد اعتماد داخلی توابع امنیتی هدف ارزیابی	راه‌اندازی یک کانال امن پایان کانال امن	شناسایی راه‌انداز و مقصد تلاشی که در برقراری یک

			شکست در عملکرد کانال امن	کانال امن، با شکست مواجه شده است
	FTP_TRP.1	مسیر مطمئن	راه‌اندازی یک کانال امن پایان کانال امن شکست در عملکرد مسیر امن	شناسایی، شناسه‌ی کاربری ادعاشده

جدول ۱:رخدادهای قابل ممیزی

نام کلاس	نام عنصر		توضیحات
هانی پات با تعامل کم	HONEYPOT_SDC.1	مجموعه داده‌های سیستم	مجموعه داده‌های سیستم
	HONEYPOT_RCT.1	واکنش تشخیص نفوذ	واکنش تحلیل‌گر

جدول ۲: الزامات کارکرد امنیتی هدف ارزیابی

۵,۱ کلاس ممیزی امنیت

شماره الزام	نام خانواده	عنصر امنیتی
۱	تولید داده ممیزی امنیت	**نام عنصر: تولید داده ممیزی امنیتی ۱**

(FAU_GEN) **شماره مؤلفه: م‌ا–ت‌ل.۱٫۱(FAU_GEN.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به تولید رکورد ممیزی از رخدادهای قابل ممیزی زیر باشد:

– کلی: ورود به سیستم کاربر، خروج از سیستم کاربر

– مدیریت کاربر: تغییر و به‌روزرسانی و تنظیم مجدد داده‌های احراز هویت، مشاهده و جستجو فهرست‌های کاربران و جزئیاتشان؛ ایجاد و به‌روزرسانی و حذف کاربران؛ مشاهده، ایجاد، به‌روزرسانی و حذف گروه‌ها

– پیکربندی: مشاهده و ذخیره‌ی پیکربندی سامانه‌ها؛ ذخیره و بازیابی تنظیمات سیستم؛ مشاهده، ایجاد، به‌روزرسانی و حذف دسته‌بندی‌های IP؛ مشاهده و ذخیره تنظیمات شبکه؛ مشاهده و پشتیبان گیری یا بازیابی فایل‌های پیکربندی

– تحلیل لاگ‌ها: مشاهده، جستجو، ایجاد، به‌روزرسانی، کپی، صدور، حذف لاگ‌های تحلیل‌شده

– شروع خودآزمایی هدف ارزیابی

– شروع و متوقف نمودن سرویس‌ها (در صورت وجود)، اضافه و حذف حس‌گرها، شروع، پایان سرویس‌ها در حس‌گرها

– [انتخاب: هیچ اقدام دیگر، [اختصاص: **لیست از دیگر رخدادها**]]

– به‌طور مشخص رویدادهای قابل ممیزی تعریف‌شده و فهرست شده در جدول۱

نکته کاربردی:

در صورت ناکامل بودن لیست مطرح‌شده در این الزام از دیدگاه نویسنده سند هدف امنیتی، لازم است با بهره بردن از «اختصاص»، دیگر رخدادهای امنیتی را لیست نمود

لازم به ذکر است نویسنده سند هدف امنیتی باید در بخش «خلاصه مشخصات هدف ارزیابی[1]» از سند هدف امنیتی، اطلاعات لاگ گرفته‌شده را مشخص نماید.

اصطلاح «سرویس» در این الزام اشاره به کانال‌ها و مسیرهای ارتباطی مورد اعتماد، خودآزمایی بنا به تقاضا، به‌روزرسانی امن و نشست‌های سرپرست (که تحت مسیر مورد اعتماد است) دارد.

۲ **نام عنصر: تولید داده ممیزی امنیتی ۱**

[1] فصلی از سند هدف امنیتی است.

شماره مؤلفه: ما-ت‌ل.۲,۱(FAU_GEN.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید در هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:

- تاریخ و زمان رخداد، نوع رخداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رخداد
- برای هر نوع رخداد ممیزی، با توجه به تعریف رخدادهای قابل ممیزی در پروفایل حفاظتی/سند هدف امنیتی [**اطلاعاتی که در ستون ۳ جدول ۱ مشخص‌شده است**].

نکته کاربردی:

همچون الزام قبلی، نویسنده سند هدف امنیتی می‌تواند جدول ۱ را با هر نوع اطلاعات تولیدشده به‌روزرسانی نماید.

نام عنصر: تولید داده ممیزی امنیتی ۲

شماره مؤلفه: ما-ت‌ل.۱,۲(FAU_GEN.2.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به مرتبط ساختن هر رویداد ممیزی با هویت کاربری که باعث ایجاد آن رویداد شده است، باشند.

نام عنصر: بازبینی ممیزی امنیت ۱

شماره مؤلفه: م‌ا–ب‌ز.۱،۱(FAU_SAR.1.1)

شرح مؤلفه:

۴

توابع امنیتی هدف ارزیابی باید[اختصاص: **کاربرانی مجاز**] برای قابلیت خواندن [اختصاص: **فهرستی از اطلاعات ممیزی**] از رکوردهای ممیزی فراهم نماید.

بازبینی ممیزی امنیت
(FAU_SAR)

نام عنصر: بازبینی ممیزی امنیت ۱

شماره مؤلفه: م‌ا–ب‌ز.۲،۱ (FAU_SAR.1.2)

۵

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به شکل مناسبی برای کاربر، جهت تفسیر اطلاعات فراهم

نماید.

نام عنصر: بازبینی ممیزی امنیت ۱

شماره مؤلفه: ما-ب‌ز.۱,۲(FAU_SAR.2.1)

شرح مؤلفه:

۶

توابع امنیتی هدف ارزیابی باید از دسترسی کلیه کاربران جهت خواندن رکوردهای ممیزی ممانعت نماید، به‌جز کاربرانی که به آن‌ها مجوز دسترسی با قابلیت خواندن داده‌شده باشد

نام عنصر: ممیزی انتخابی ۱

شماره مؤلفه: ما-اخ.۱,۱(FAU_SEL.1.1)

شرح مؤلفه:

۷ انتخاب رویداد ممیزی امنیت **(FAU_SEL)**

توابع امنیتی هدف ارزیابی باید قابلیت انتخاب رویدادهای قابل ممیزی را بر اساس دارا بودن/نبودن ویژگی‌های زیر از مجموعه رویدادهای ممیزی داشته باشند:

الف- نوع رویداد

ب- [اختصاص: **فهرستی از ویژگی‌های تکمیلی که انتخاب ممیزی بر اساس آن است**].

نام عنصر: ذخیره‌سازی رخدادهای ممیزی امنیت ۱

شماره مؤلفه: م‌ا-ذخ-(ت‌س).۱,۱(FAU_STG_EXT.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به ارسال داده ممیزی تولیدشده به یک موجودیت IT خارجی از طریق کانال مورد اعتماد مطابق با FTP_ITC.1.1 باشد.

۸	ذخیره‌سازی ممیزی امنیت **(FAU_STG)**	رویدادهای

نکته کاربردی:

برای انتخاب گزینه «انتقال داده ممیزی به خارج از موجودیت IT» هدف ارزیابی برای ذخیره و بازبینی رکوردهای ممیزی به یک سرور ممیزی غیر هدف ارزیابی وابسته است.

۹ **نام عنصر: ذخیره‌سازی رخدادهای ممیزی امنیت ۱**

شماره مؤلفه: ما-ذخ-(ت‌س).۲,۱.(FAU_STG_EXT.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به ذخیره کردن داده ممیزی در خود هدف ارزیابی باشد.

نام عنصر: ذخیره‌سازی رخدادهای ممیزی امنیت ۱

شماره مؤلفه: ما-ذخ-(ت‌س).۳,۱.(FAU_STG_EXT.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر [انتخاب: حذف داده ممیزی جدید، بازنویسی رکوردهای ممیزی پیشین مطابق با قوانین زیر باشد: [اختصاص: **قوانین برای بازنویسی رکوردهای ممیزی پیشین**]، [اختصاص: **دیگر اقدامات**]] وقتی فضای ذخیره‌سازی محلی برای داده ممیزی پرشده است.

نکته کاربردی:

در شرایطی که فضای ذخیره‌سازی محلی پر است ممکن است از سرور لاگ خارجی به عنوان فضای ذخیره‌سازی جایگزین استفاده گردد. از «دیگر اقدامات» در این مورد می‌توان به «فرستادن داده ممیزی جدید به موجودیت

IT خارجی» اشاره نمود.

نام عنصر: تضمین در دسترس بودن داده‌های ممیزی ۲

شماره مؤلفه: م‌ا–ذخ.۱,۲(FAU_STG.2.1)

شرح مؤلفه:

۱۱	ذخیره‌سازی ممیزی امنیت **(FAU_STG)**	رویدادهای

توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی ذخیره‌شده را از حذف غیرمجاز محافظت نماید.

۵,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام خانواده	عنصر امنیتی

نام عنصر: تولید کلید رمزنگاری ۱

شماره مؤلفه: رز–م‌ک.۱,۱ (FCS_CKM.1.1)

شرح مؤلفه:

۱۲	مدیریت کلید رمزنگاری **(FCS_CKM)**	

توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد زیر

شماره الزام	نام خانواده	عنصر امنیتی

تولید کنند.

[انتخاب:

- *استفاده از طرح RSA با اندازه کلید 2048 بیت یا بیشتر که از این موارد پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.3*
- *استفاده از طرح ECC "NIST curves" [انتخاب: P-256، P-384 ، P-521] که از موارد زیر پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.4*
- *استفاده از طرح رمزنگاری FFC با اندازه کلید ۲۰۴۸ بیت یا بیشتر که از موارد زیر پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.1*

نکته کاربردی:

نویسنده سند هدف امنیتی تمام طرح‌های تولید کلید که برای استقرار و احراز هویت تجهیزات استفاده می‌شود را انتخاب می‌کند. وقتی تولید کلید برای استقرار کلید استفاده می‌شود، طرح‌ها در الزام FCS_CKM.2.1 و پروتکل‌های رمزنگاری انتخاب‌شده باید منطبق باشد. وقتی کلید تولیدشده برای احراز هویت تجهیزات استفاده

شماره الزام	نام خانواده	عنصر امنیتی
		می‌شود، انتظار می‌رود کلید عمومی با یک گواهی X.509v3 مرتبط گردد.
		در صورتی که هدف ارزیابی به عنوان یک گیرنده در طرح استقرار کلید RSA عمل نماید، نیاز به پیاده‌سازی تولید کلید RSA نیست.
		نام عنصر: استقرار کلید رمزنگاری ۲
		شماره مؤلفه: رز-م‌ک.۱,۲ (FCS_CKM.2.1)
۱۳		**شرح مؤلفه:**
		توابع امنیتی هدف ارزیابی باید استقرار کلید رمزنگاری را مطابق با یک روش استقرار کلید رمزنگاری مشخص انجام دهد: [انتخاب:
		• طرح استقرار کلید مبتنی بر RSA که از استاندارد زیر پیروی می‌کند:

شماره الزام	نام خانواده	عنصر امنیتی

NIST Special Publication 800-56B، «توصیه‌نامه برای طرح‌های استقرار کلید دوبه‌دو با استفاده از رمزنگاری تجزیه به عوامل صحیح[1]»

- طرح استقرار کلید مبتنی بر منحنی بیضوی که از استاندارد زیر پیروی می‌کند:

NIST Special Publication 800-56A، «توصیه‌نامه برای طرح‌های استقرار کلید دوبه‌دو با استفاده از رمزنگاری لگاریتم گسسته[2]»

- طرح استقرار کلید مبتنی بر میدان متناهی که از استاندارد زیر پیروی می‌کند:

NIST Special Publication 800-56A، «توصیه‌نامه برای طرح‌های استقرار کلید دوبه‌دو با استفاده از رمزنگاری لگاریتم گسسته»

]

نکته کاربردی:

این الزام FCS_CKM.2 است که به‌جای توزیع کلید برای استقرار کلید از آن استفاده‌شده است. نویسنده سند

[1] Integer Factorosation Cryptography

[2] Discrete Logarithm Cryptography

شماره الزام	نام خانواده	عنصر امنیتی
		هدف امنیتی با توجه به پروتکل‌های رمزنگاری انتخاب‌شده، طرح‌های استقرار کلید را انتخاب می‌نماید. طرح‌های استقرار کلید مبتنی بر RSA در بخش نهم از استاندارد NIST SP 800-56B شرح داده‌شده است. هرچند بخش نهم از استاندارد متکی بر پیاده‌سازی دیگر بخش‌ها در SP 800-56B است. در صورتی که هدف ارزیابی به عنوان گیرنده در طرح برقراری کلید RSA عمل نماید، هدف ارزیابی نیازی به پیاده‌سازی تولید کلید RSA ندارد. منحنی‌های بیضوی که برای طرح برقراری کلید استفاده می‌شود با منحنی مشخص‌شده در الزام FCS_CKM.1.1 همبسته می‌شود. دامنه پارامترهای استفاده‌شده برای طرح استقرار کلید مبتنی بر میدان متناهی توسط الزام FCS_CKM.1.1 مشخص می‌گردد.
		نام عنصر: تخریب کلید رمزنگاری ۴
۱۴		**شماره مؤلفه: رز-م‌ک.۱,۴ (FCS_CKM.4.1)**
		شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری را مطابق با روش‌های تخریب کلید رمزنگاری مشخص تخریب نماید [انتخاب:

- برای حافظه فرار، تخریب باید به‌وسیله یک تک جایگزینی مستقیم متشکل از [انتخاب: یک الگو شبه تصادفی با استفاده از تولید بیت تصادفی، صفرها] اجرا شود، به دنبال آن باید با خواندن حافظه وارسی و تائید صورت گیرد.

  در صورتی که در وارسی، خواندن داده رونویسی شده با خطا مواجه شود، فرآیند باید دوباره تکرار شود.
- برای حافظه غیر فرار EEPROM، تخریب باید به‌وسیله یک، بازنویسی مستقیم متشکل از الگوی شبه تصادفی با استفاده از تولید بیت تصادفی (مشخص‌شده در الزام FCS_RBG_EXT.1) اجرا شود، و به دنبال آن باید با خواندن حافظه وارسی و تائید صورت گیرد.

  در صورتی که در وارسی، خواندن داده رونویسی شده با خطا مواجه شود، فرآیند باید دوباره تکرار شود.
- برای حافظه فلش غیر فرار، تخریب باید به‌وسیله [انتخاب: جایگزینی مستقیم شامل صفرها، پاک کردن بلوک] اجرا شود، و به دنبال آن باید با خواندن حافظه وارسی و تائید صورت گیرد.

شماره الزام	نام خانواده	عنصر امنیتی
		در صورتی که در وارسی، خواندن داده رونویسی شده با خطا مواجه شود، فرآیند باید دوباره تکرار شود.
		• برای یک حافظه غیر فرار به‌جز EEPROM و فلش، تخریب باید به‌وسیله سه یا بیشتر از سه بار جایگزینی با الگوی تصادفی که قبل از هر نوشتن تغییر می‌کند اجرا شود.
		[
		نام عنصر: عملیات رمزنگاری (رمزنگاری/رمزگشایی AES) ۱(۱)
		شماره مؤلفه: رز-ع‌ر.۱٫۱(۱) (FCS_COP.1.1(1))
		شرح مؤلفه:
۱۵	عملیات رمزنگاری (**FCS_COP**)	توابع امنیتی هدف ارزیابی باید [رمزنگاری و رمزگشایی] را مطابق با الگوریتم رمزنگاری AES که از مدهای [انتخاب: CBM، GCM] استفاده می‌کند و اندازه کلید رمزنگاری [انتخاب:۱۲۸ بیت، ۱۹۲ بیت، *۲۵۶ بیت*] مطابق با: *AES مشخص‌شده در استاندارد ISO 18033-3*، [انتخاب: CBC مشخص‌شده در استاندارد ISO 10116، GCM مشخص‌شده در استاندارد ISO 19772] انجام دهند.

شماره الزام	نام خانواده	عنصر امنیتی

نکته کاربردی:

برای اولین انتخاب از FCS_COP.1.1(1)، نویسنده سند هدف امنیتی باید مد یا مدهای که در عملگرهای AES است را انتخاب کند. برای دومین انتخاب، نویسنده سند هدف امنیتی باید اندازه کلیدهای پشتیبانی شده را انتخاب کند.

نام عنصر: عملیات رمزنگاری (تولید و وارسی امضا) ۱(۲)

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

شرح مؤلفه:

1 ۱۶ توابع امنیتی هدف ارزیابی باید خدمات رمزنگاری امضا را مطابق با الگوریتم‌های رمزنگاری [انتخاب:

- الگوریتم امضای دیجیتال RSA با اندازه کلید رمزنگاری [اختصاص: ۲۰۴۸ بیت یا بیشتر]
- الگوریتم امضای دیجیتال منحنی بیضوی و اندازه کلید رمزنگاری [اختصاص: ۲۵۶ بیت یا بیشتر]

شماره الزام	نام خانواده	عنصر امنیتی

[

انجام دهد، الگوریتم امضاء دیجیتال برآورده‌کننده زیر است:

[اختصاص:

- برای طرح RSA: FIPS PUB 186-4 «استاندارد امضاء دیجیتال (DSS)»، بخش ۵,۵، با استفاده از طرح-های امضاء RSASSA-PSS یا RSASSA-PKCS2v1_5 از PKCS #1 v2.1؛ ISO/IEC 9796-2 «طرح امضاء دیجیتال ۲ یا ۳»

- برای طرح ECDSA: FIPS PUB 186-4 «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، پیاده‌سازی «منحنی بیضوی» P-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ استاندارد ISO/IEC 14888-3 بخش ۶,۴

]

نکته کاربردی:

نویسنده سند هدف امنیتی برای امضاء دیجیتال، الگوریتم پیاده‌سازی شده‌ای را انتخاب می‌نماید. برای الگوریتم

شماره الزام	نام خانواده	عنصر امنیتی
		انتخاب‌شده باید پارامترهای مناسبی تعیین می‌گردد.
		نام عنصر: عملیات رمزنگاری (الگوریتم درهم‌سازی ۱(۳)
		شماره مؤلفه: رز-ع‌ر.۱٫۱(۳) (FCS_COP.1.1(3))
		شرح مؤلفه:
۱۷		توابع امنیتی هدف ارزیابی باید به‌منظور [خدمات درهم‌سازی] از الگوریتم رمزنگاری [انتخاب:*SHA-1*، *SHA-256, SHA-384, SHA-512*] مطابق با استاندارد *ISO/IEC 10118-3:2004* استفاده نمایند.
		نکته کاربردی:
		توصیه می‌شود تولیدکنندگان محصول پروتکل‌های بروز شده‌ای را پیاده‌سازی کنند که از خانواده SHA-2 پشتیبانی نمایند؛ تا زمان پشتیبانی از پروتکل‌های بروز شده، این پروفایل اجازه پشتیبانی از پیاده‌سازی الگوریتم SHA-1 مطابق با SP 800-131A می‌دهد.
		درهم‌سازی انتخاب‌شده باید با قدرت الگوریتم مورداستفاده در الزامات FCS_COP.1(1) و FCS_COP.1(2)

شماره الزام	نام خانواده	عنصر امنیتی
		منطبق باشد. (برای مثال، SHA 256 برای کلیدهای ۱۲۸ بیتی)
۱۸		**نام عنصر: عملیات رمزنگاری (الگوریتم درهم‌سازی مبتنی بر کلید) ۱(۴))** **شماره مؤلفه: رز-ع‌ر.۱٫۱(۴) ((FCS_COP.1.1(4))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید احراز هویت پیام با استفاده از درهم‌سازی مبتنی بر کلید را مطابق با الگوریتم رمزنگاری [[انتخاب:*SHA-256, SHA-384, SHA-512*]-HMAC[]، اندازه کلید [اختصاص: **اندازه کلید (بیت) استفاده‌شده در HMAC**] و اندازه‌ی چکیده پیام [اختصاص: ۱۶۰، ۲۵۶، ۳۸۴ و ۵۱۲ بیت] مطابق با *ISO/IEC 9797*-2:2011، بخش ۷ «الگوریتم MAC 2»، انجام دهند. **نکته کاربردی:** اندازه کلید در قسمت «اختصاص» در محدوده بین L1 و L2 قرار می‌گیرد (تعریف‌شده در ISO/IEC10118 برای توابع درهم‌ساز مناسب). به عنوان مثال برای الگوریتم SHA-256، L1=512 و L2=256 است، بنابراین اندازه

شماره الزام	نام خانواده	عنصر امنیتی
		کلید بین L1 وL2 است. (L2<=K<=L1)
		نام عنصر: تولید بیت تصادفی ۱
		شماره مؤلفه: رز-بت-(ت‌س).۱,۱ (FCS_RBG_EXT.1.1)
		شرح مؤلفه:
۱۹	تولید بیت تصادفی (FCS_RBG_EXT)	توابع امنیتی هدف ارزیابی باید تمام خدمات تولید بیت تصادفی قطعی را مطابق با ISO/IEC 18031:2011با استفاده از [انتخاب: Hash_DRBG(any)،HMAC_DRBG(any)،CTR_DRBG(AES)] انجام دهند.
		نام عنصر: تولید بیت تصادفی ۱
		شماره مؤلفه رز-بت-(ت‌س).۲,۱ (FCS_RBG_EXT.1.2)
۲۰	تولید بیت تصادفی (FCS_RBG_EXT)	**شرح مؤلفه:** تولید بیت تصادفی قطعی باید حداقل توسط یک منبع آنتروپی تغذیه شود که آنتروپی آن از [انتخاب: [اختصاص: **تعدادی از منابع مبتنی بر نرم‌افزار**]، منبع نویز مبتنی بر نرم‌افزار،[اختصاص: **تعدادی از منابع مبتنی بر**

شماره الزام	نام خانواده	عنصر امنیتی

سخت‌افزار]،منبع نویز مبتنی بر سخت‌افزار] با حداقل [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] از آنتروپی حداقل برابر بزرگ‌ترین قدرت امنیتی، مطابق با جدول C.1 از استاندارد ISO/IEC 18031:2011 با عنوان «جدول قدرت امنیتی برای توابع درهم سازی»، کلیدها و درهم‌سازی‌ها تولید خواهد شد.

نکته کاربردی:

برای اولین انتخاب در FCS_RBG_EXT.1.2، نویسنده سند هدف امنیتی حداقل یکی از انواع منابع نویز را انتخاب می‌نماید. اگر هدف ارزیابی شامل چندین منبع نویز همنوع باشد، نویسنده سند هدف امنیتی قسمت «الزام» را با تعداد مناسبی برای هر نوع منبع کامل می‌نماید (به عنوان مثال، ۲ منبع نویز مبتنی بر نرم‌افزار، ۱ منبع نویز مبتنی بر سخت‌افزار).

استاندارد ISO/IEC 18031:2011 شامل ۳ روش متفاوت برای تولید عدد تصادفی است: هرکدام از این‌ها، به‌نوبه خود، وابسته به پارامترهای درونی رمزنگاری است (توابع درهم سازی /رمز).

نویسنده سند هدف امنیتی تابع استفاده‌شده را انتخاب و پارامترهای درونی رمزنگاری استفاده‌شده در این الزام را

شماره الزام	نام خانواده	عنصر امنیتی

در نظر می‌گیرد. درحالی‌که هر یک از توابع درهم سازی شناخته‌شده (SHA-1،SHA-224،SHA-256،SHA-512،384) برای Hash-DRBG یا HMAC-DRBG مجاز هستند، تنها پیاده‌سازی بر اساس AES برای CTR-DRBG مجاز است.

در صورتی که طول کلید برای پیاده‌سازی AES استفاده‌شده در این الزام متفاوت از طول کلیدی باشد که برای رمزنگاری داده کاربری استفاده می‌شود، بنابراین می‌توان الزام FCS_COP.1 در سند هدف امنیتی با طول کلید متفاوت تکرار نمود.

برای انتخاب در FCS_RBG_EXT.1.2، نویسنده هدف امنیتی باید تعداد حداقل بیت‌های آنتروپی که برای تولید بیت تصادفی استفاده می‌شود را انتخاب نماید.

۵,۳ کلاس حفاظت از داده‌های کاربری[1]

شماره الزام	نام خانواده	عنصر امنیتی
		نام عنصر: حفاظت کامل از داده‌های باقی‌مانده ۲
		شماره مؤلفه: ح‌ف-اب.۱,۲(FDP_RIP.2.1)
۲۱	حفاظت از داده‌های باقی‌مانده **(FDP_RIP)**	**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تضمین نمایند که هرگونه محتوی اطلاعات قبلی یک منبع را در زمان [انتخاب: *تخصیص منابع به، آزادسازی منابع از*] تمام موجودیت‌های غیرفعال، غیرقابل‌دسترس نمایند.

1 User data protection(FDP)

۵,۴ کلاس شناسایی و احراز هویت[1]

شماره الزام	نام خانواده	عنصر امنیتی
۲۲	مدیریت رمز عبور (FIA_PMG_EXT)	**نام عنصر: مدیریت رمز عبور ۱** **شماره مؤلفه: اش-م‌ع.۱,۱.۱ (FIA_PMG_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت‌های مدیریت رمز عبور را که در زیر ذکرشده‌اند برای رمزهای عبور سرپرستی فراهم نماید: ۱ رمزهای عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: *"@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" ,")" [الزام: **کاراکتر دیگر***]] باشند. ۲ حداقل طول رمز عبور باید توسط سرپرست امنیت، قابل تنظیم بوده و۱۵کاراکتر یا بیشتر باشد.

[1] Identification and authentication(FIA)

نکته کاربردی:

نویسنده‌ی سند هدف امنیتی، کاراکترهای خاصی را که توسط هدف ارزیابی پشتیبانی می‌گردند انتخاب می-نماید. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» لیست نماید. «رمز عبور سرپرستی» به آن دسته از رمز عبورهایی اشاره دارد، که سرپرستان از آن‌ها در کنسول محلی یا پروتکل‌هایی که از رمز عبور پشتیبانی می‌نمایند (همچون SSH,HTTPS)، استفاده می‌کنند.

نام عنصر: شناسایی و احراز هویت کاربر ۱

شماره مؤلفه: اش-ش‌ه.۱,۱ (FIA_UIA_EXT.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید پیش از آنکه به موجودیت‌های غیر هدف ارزیابی، جهت شروع رویه شناسایی و احراز هویت نیاز باشد، اقدامات زیر را مجاز نماید:

۲۳	شناسایی و احراز هویت کاربر **(FIA_UIA_EXT)**	• نمایش هشدارها مطابق با خانواده «FTA_TAB.1» • [انتخاب: *بدون هیچ اقدام دیگر*، *[اختصاص:* ***فهرستی از سرویس‌ها، اقداماتی که توسط توابع امنیتی هدف ارزیابی جهت پاسخ دادن به درخواست‌های «غیر هدف ارزیابی» صورت می-گیرد****]]

نام عنصر: شناسایی و احراز هویت کاربر ۱

شماره مؤلفه: اش-ش‌ه.۲٫۱ (FIA_UIA_EXT.1.2)

شرح مؤلفه:

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

نکته کاربردی:

۲۴

این الزامات به کاربران سرویس‌هایی اعمال می‌گردد که از هدف ارزیابی مستقیماً قابل‌دسترس است و شامل سرویس‌هایی که با اتصال از طریق هدف ارزیابی در دسترس قرار می‌گیرند، نمی‌شود. در حالی که باید هیچ سرویس و یا سرویس‌های کمی پیش از شناسایی و احراز هویت در دسترس موجودیت‌های خارجی باشند، در صورت وجود چنین سرویس‌هایی باید در قسمت «اختصاص» لیست گردند، در غیر این صورت «بدون هیچ اقدام دیگر» انتخاب می‌شود.

احراز هویت می‌تواند بر اساس کلمه عبور از طریق یک کنسول محلی یا پروتکلی که از چنین رمزهای عبوری پشتیبانی می‌نماید (همچون SSH)، یا بر اساس گواهینامه (SSH,TLS) باشد.

برای ارتباط با یک موجودیت IT خارجی (برای مثال سرور ممیزی، یا NTP سرور) چنین اتصالاتی باید مطابق با عنصر FTP_ITC صورت گیرد.

نام عنصر: سازوکار احراز هویت بر اساس رمز عبور ۲

شماره مؤلفه: اش-اه.۱,۲ (FIA_UAU_EXT.2.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی جهت احراز هویت سرپرستان، باید یک سازوکار احراز هویت محلی مبتنی بر رمز عبور [انتخاب: *[اختصاص: **دیگر سازوکارهای احراز هویت**]*، *هیچ‌کدام*] فراهم نماید.

۲۵

احراز هویت کاربر (**FIA_UAU**)

نکته کاربردی:

در قسمت «اختصاص» هر سازوکار احراز هویت محلی دیگری که پشتیبانی شده است معرفی می‌شود. از جمله سازوکارهای احراز هویت محلی می‌توان به آن‌هایی که از طریق کنسول محلی استفاده می‌شود اشاره نمود. نشست‌های سرپرستی از راه دور (و سازوکارهای احراز هویت مرتبط آن‌ها) در FTP_TRP.1 مشخص می‌شود.

۲۶

نام عنصر: بازخورد احراز هویت محافظت‌شده ۷

شماره مؤلفه: اش-اه.۱,۷ (FIA_UAU.7.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید زمانی که فرآیند احراز هویت، در کنسول محلی در حال صورت گرفتن است؛ تنها به سرپرست بازخورد مبهمی[1] ارائه دهند.

نکته کاربردی:

«بازخورد مبهم نشان می‌دهد که توابع امنیتی هدف ارزیابی، از هر داده‌ای که توسط کاربر جهت احراز هویت کاربر وارد می‌شود، نمایش واضحی ندارند(مانند انعکاس رمز عبور). هرچند ممکن است از روند احراز هویت «بازخورد مبهم» ارائه گردد(همچون * که در زمان وارد نمودن هر کاراکتر توسط کاربر، نشان داده می‌شود). اما این بازخورد هیچ اطلاعاتی را در طول رویه احراز هویت به کاربر برنمی‌گرداند.

۲۷

نام عنصر: احراز هویت با استفاده از گواهینامه‌های X.509

شماره مؤلفه: اش-اگ.۱,۷ (FIA_X509.EXT.1)

شرح مؤلفه:

[1] Obscured feedback

توابع هدف ارزیابی باید اعتبارسنجی را مطابق با قوانین زیر انجام دهد:

- اعتبارسنجی گواهینامه RFC 5280 و اعتبارسنجی مسیر گواهینامه
- مسیر گواهینامه باید با یک گواهینامه CA مورد اعتماد خاتمه یابد.
- توابع هدف ارزیابی باید مسیر گواهینامه را به‌وسیله اطمینان از وجود افزونه basicConstraintها که پرچم CA برای گواهینامه‌های CA با مقدار TRUE قرار داده‌شده است، اعتبارسنجی نماید.
- توابع هدف ارزیابی باید وضعیت ابطال گواهی‌ها را با استفاده از [انتخاب: پروتکل وضعیت گواهینامه آنلاین (OCSP) همان‌طور که در RFC 2560 مشخص‌شده است، لیست ابطال گواهینامه CRL همان‌طور که در RFC 5759 مشخص‌شده است] مشخص نماید.
- توابع هدف ارزیابی باید فیلد extendedKeyUsage را مطابق با قوانین زیر اعتبارسنجی کند:
  - گواهینامه‌ها برای به‌روزرسانی مورد اعتماد و اعتبارسنجی صحت کدهای اجرا باید هدف امضای کد *(id-kp 3 with OID 1.3.6.1.5.5.7.3.3)* را در فیلد extendedKey داشته باشد.

- گواهینامه‌ها سرور برای TLS جهت احراز هویت سرور (*id-kp 1 with OID 1.3.6.1.5.5.7.3.1*) در فیلد extendedKeyUsage باید باشد.
- گواهینامه‌ها مشتری برای TLS جهت احراز هویت مشتری (*id-kp 2 with OID 1.3.6.1.5.5.7.3.2*) در فیلد extendedKeyUsage باید باشد.
- گواهینامه‌های OCSP برای پاسخ‌های OCSP با هدف امضای OCSP (*id-kp 9 with OID 1.3.6.1.5.5.7.3.9*) در فیلد extendedKeyUsage ارائه شود.

۵,۵ کلاس مدیریت امنیت۱

شماره الزام	نام خانواده	عنصر امنیتی
۲۸		**نام عنصر: مدیریت رفتار توابع امنیتی هدف ارزیابی(به‌روزرسانی) ۱** **شماره مؤلفه: م‌د-م‌د.۱,۱ (FMT_MOF.1.1(1)/TrustedUpdate)**

1 Functional Security management (FMT)

شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: توابع امنیتی هدف ارزیابی باید امکان فعال‌سازی توابع برای انجام به‌روزرسانی [انتخاب: آفلاین، آنلاین] را فقط به سرپرستان مجاز محدود کند. **نکته کاربردی:** در این الزام باید شروع به‌روزرسانی به سرپرست مجاز محدود گردد.
۲۹	مدیریت داده‌های امنیتی هدف ارزیابی (**FMT_MTD**) توابع	**نام عنصر: مدیریت داده‌های توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: م‌د-م‌د.۱,۱.۱ (FMT_MTD.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید امکان **مدیریت** داده‌های توابع امنیتی هدف ارزیابی را تنها به سرپرست امنیتی محدود نماید. **نکته کاربردی:**

شماره الزام	نام خانواده	عنصر امنیتی
		عبارت **مدیریت** اشاره به «ایجاد، مقداردهی، مشاهده، تغییر پیش‌فرض، تغییر دادن،-حذف نمودن، پاک کردن و اضافه نمودن» داده‌ها دارد؛ اما تنها به این موارد نیز محدود نمی‌گردد. از جمله داده‌های توابع امنیتی هدف ارزیابی می‌توان به «اطلاعات رمزنگاری» اشاره نمود. تنظیم مجدد کلمه عبور توسط سرپرست نمونه‌ای از این الزام است.
۳۰	مشخصات کارکردهای مدیریتی **(FMT_SMF)**	**نام عنصر: مشخصات کارکردهای مدیریتی ۱** **شماره مؤلفه: م‌د-ع‌م.۱،۱ (FMT_SMF.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قادر به انجام کارکردهای مدیریتی زیر باشد: • قابلیت سرپرستی نمودن هدف ارزیابی به‌صورت محلی و از راه دور • قابلیت پیکره‌بندی بنرهای دسترسی • قابلیت پیکره‌بندی زمان نشست‌های محاوره‌ای قبل از خاتمه نشست یا قفل شدن.

شماره الزام	نام خانواده	عنصر امنیتی

- قابلیت به‌روزرسانی هدف ارزیابی و تائید صحت به‌روزرسانی با استفاده از روش [انتخاب: *امضاء دیجیتال*، *کد درهم سازی منتشرشده، بدون سازوکار دیگر*] پیش از آنکه به‌روزرسانی نصب گردد.
- *ورود کاربر به سیستم؛ خروج کاربر از سیستم*
- مدیریت کاربر: تغییر و به‌روزرسانی و تنظیم مجدد داده‌ی احراز هویت، مشاهده و جستجو فهرست‌های کاربران و جزئیاتشان؛ ایجاد و به‌روزرسانی و حذف کاربران؛ مشاهده، ایجاد، به‌روزرسانی و حذف گروه‌ها؛
- پیکربندی: مشاهده و ذخیره‌ی پیکربندی سامانه‌ها؛ ذخیره و بازیابی تنظیمات سیستم؛ مشاهده، ایجاد، به‌روزرسانی و حذف دسته‌بندی‌های IP؛ مشاهده و ذخیره تنظیمات شبکه؛
- [انتخاب:
  - *قابلیت پیکره‌بندی رفتارهای ممیزی*
  - *قابلیت پیکربندی فهرستی از سرویس‌های در دسترس ارائه‌شده توسط هدف ارزیابی، پیش از شناسایی و احراز هویت یک موجودیت به‌صورت مشخص‌شده در الزام.FIA_UIA_EXT*
  - *قابلیت پیکربندی توابع رمزنگاری*

شماره الزام	نام خانواده	عنصر امنیتی

- *بدون هیچ قابلیت دیگری*
- [اختصاص: **دیگر کارکردهای مدیریتی**]

]

نکته کاربردی:

هدف ارزیابی باید قابلیتی برای سرپرستی از راه دور و محلی ایجاد نماید تا از آن طریق نسبت به دریافت به‌روزرسانی‌ها از منبع امن اطمینان حاصل گردد. سرپرست باید بتواند این‌گونه اقدامات را با استفاده از امضاء دیجیتال و کد درهم‌سازی منتشرشده انجام دهند. نویسنده سند هدف امنیتی، در اولین «انتخاب» باید مشخص نماید به‌روزرسانی‌ها چگونه تائید می‌گردند، هر انتخاب در این قسمت باید با انتخاب در الزام FPT_TUD_EXT.1 مطابقت داشته باشد.

در دومین «انتخاب» در صورتی «*قابلیت پیکره‌بندی رفتارهای ممیزی*» انتخاب می‌گردد که هدف ارزیابی امکان پیکربندی سرویس‌های در دسترس را پیش از شناسایی و احراز هویت برای سرپرست فراهم نماید.

دومین مورد در صورتی انتخاب می‌گردد که هر عملکرد رمزنگاری بر روی هدف ارزیابی را بتواند پیکربندی نماید،

شماره الزام	نام خانواده	عنصر امنیتی
		در غیر این صورت عبارت «بدون هیچ قابلیت دیگری» را انتخاب می‌گردد.
		نام عنصر: محدودسازی نقش‌های امنیتی ۲
		شماره مؤلفه: م‌د-ن‌م.۱,۲(FMT_SMR.2.1)
		شرح مؤلفه:
۳۱	نقش‌های امنیت (**FMT_SMR**)	توابع امنیتی هدف ارزیابی، باید نقش‌های زیر را نگهداری نمایند: • سرپرست امنیتی • [اختصاص: **دیگر نقش‌ها**]
		نام عنصر: محدودسازی نقش‌های امنیتی ۲
		شماره مؤلفه: م‌د-ن‌م.۲,۲(FMT_SMR.2.2)
۳۲		**شرح مؤلفه:**
		توابع امنیتی هدف ارزیابی باید قادر به مرتبط نمودن کاربران با نقش‌هایشان باشند.

شماره الزام	نام خانواده	عنصر امنیتی
		نکته کاربردی: لازم است حساب‌های کاربری تنها با یک نقش مرتبط شده باشند. هرچند ممکن است چندین کاربر نقش مشابهی داشته باشند و نیازی نیست که هدف ارزیابی نقش‌ها را تنها به یک کاربر محدود نماید.
۳۳		**نام عنصر: محدودسازی نقش‌های امنیتی ۲** **شماره مؤلفه: م‌د-ن‌م.۳,۲(FMT_SMR.2.3)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تضمین نمایند که شرایط زیر برآورده می‌شوند: • نقش سرپرست مجاز امنیتی باید قادر به سرپرستی هدف ارزیابی به‌صورت محلی باشد. • نقش سرپرست مجاز امنیتی باید قادر به سرپرستی هدف ارزیابی به‌صورت راه دور باشد. **نکته کاربردی**: لازم است که سرپرست مجاز، قادر به سرپرستی هدف ارزیابی از طریق کنسول محلی و یا سازوکارهای راه دور

شماره الزام	نام خانواده	عنصر امنیتی
		باشد (IPsec, SSH, TLS, TLS/HTTPS)

۵,۶ کلاس حفاظت از توابع امنیتی هدف ارزیابی۱

شماره الزام	نام خانواده	عنصر امنیتی
۳۴	انتقال داده‌های داخل هدف ارزیابی **(FPT_ITT)**	**نام عنصر: محافظت از انتقال داده‌های داخل توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: حت-اد.۱,۱ (FPT_ITT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از افشاء شدن یا تغییر داده توابع امنیتی هدف ارزیابی زمانی که بین بخش‌های مجزای هدف ارزیابی منتقل می‌گردد محافظت نماید.
۳۵	محافظت از داده‌های توابع امنیتی هدف ارزیابی **(FPT_SKP_EXT)**	**نام عنصر: محافظت از داده‌های توابع امنیتی هدف ارزیابی (کلیدهای متقارن) ۱** **شماره مؤلفه: حت-مح-(ت س).۱,۱ (FPT_SKP_EXT.1.1)**

1 Protection of the TSF(FPT)

شماره الزام	نام خانواده	عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید از خوانده شدن تمام کلیدهای از پیش به اشتراک گذارده شده، کلیدهای متقارن و کلیدهای خصوصی جلوگیری نمایند.

نکته کاربردی:

منظور این الزام آن است که سرپرست قادر به مشاهده و خواندن کلیدهای شناسایی‌شده از طریق واسطهای «معمول» نیست واضح است که سرپرست می‌تواند مستقیماً حافظه را بخواند و یا کلیدها را مشاهده نماید، اما انجام این امر نیز به‌سادگی نیست. بنابراین سرپرست به عنوان یک عامل امن در نظر گرفته می‌شود که سعی در خواندن یا مشاهده کلید ندارد.

نام عنصر: حفاظت از کلمه عبور سرپرست ۱

۳۶	حفاظت از کلمه عبور سرپرست **(FPT_APW_EXT.)**	**شماره مؤلفه: ح‌ت-م‌پ-(ت س).۱,۱ (FPT_APW_EXT.1.1)**

شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی
		توابع امنیتی هدف ارزیابی نباید کلمه‌های عبور را به‌صورت متن آشکار ذخیره نمایند.
		نام عنصر: حفاظت از کلمه عبور سرپرست ۱
		شماره مؤلفه: ح‌ت-م‌پ-(ت س).۲,۱.۱ (FPT_APW_EXT.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید از خواندن کلمه‌های عبور به‌صورت متن آشکار جلوگیری نمایند.
		نکته کاربردی:
۳۷		منظور این الزام آن است که داده‌های مربوط برای احراز هویت به‌صورت متن آشکار ذخیره نگردند، و هیچ کاربر و سرپرستی قادر به خواندن کلمه عبور به‌صورت متن آشکار از طریق واسط‌های معمول نیست. سرپرست اصلی هدف ارزیابی قطعاً می‌تواند کلمه عبور را مستقیماً از حافظه بازیابی نماید، اما از آنجا که مورد اعتماد است این کار را انجام نمی‌دهد. در این نسخه از پروفایل حفاظتی الزامی بر روی روش مورداستفاده جهت ذخیره کلمه عبور به‌صورت غیر متنی وجود ندارد، اما مرجع روش‌های رمزنگاری در الزام FCS_COP پیشنهاد داده می‌شوند.

شماره الزام	نام خانواده	عنصر امنیتی
۳۸		

نام عنصر: آزمایش هدف ارزیابی

شماره مؤلفه: ح‌ت-آه-(ت س).۱,۱ (FPT_TST_EXT.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی برای نشان دادن عملکرد صحیح خود باید [انتخاب: در حین شروع راه‌اندازی، به‌صورت دوره‌ای در حین عملیات عادی، در زمان درخواست کاربر مجاز، در شرایط [اختصاص: **شرایطی که خودآزمایی باید اتفاق افتد**]]، خودآزمایی‌های [اختصاص: **فهرستی از خودآزمایی‌ها که توسط توابع امنیتی هدف ارزیابی اجرا می‌شود**] اجرا نماید.

نکته کاربردی:

انتظار می‌رود که خودآزمایی در حین شروع راه‌اندازی (در زمان شروع) انجام شود. از دیگر انتخاب‌ها تنها در شرایطی استفاده می‌شود که تولیدکننده بتواند توجیهی از عدم انجام در زمان راه‌اندازی ارائه دهد. انتظار می‌رود حداقل خودآزمایی برای بررسی صحت میان‌افزار، نرم‌افزار و همچنین برای عملکرد صحیح کارکردهای رمزنگاری در این الزام مطرح شود. در صورتی که تمام خودآزمایی‌ها در زمان شروع راه‌اندازی رخ ندهد لازم است این الزام

شماره الزام	نام خانواده	عنصر امنیتی
		با گزینه‌های مناسب تکرار شود. در صورتی که برای سازوکار خودآزمایی از گواهی استفاده شود (برای بررسی امضاء و بررسی صحت)، گواهی‌ها مطابق با الزام FIA_X509_EXT.1 اعتبارسنجی می‌شود و باید در الزام FIA_X509_EXT.2.1 انتخاب شوند. به‌علاوه الزام FPT_TST_EXT.2 باید در سند هدف امنیتی در نظر گرفته شود.
۳۹	مهرهای زمانی (FPT_STM)	**نام عنصر: مهرهای زمانی ۱** **شماره مؤلفه: ح‌ت-م‌ز.۱٫۱(FPT_STM.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید قادر به ایجاد مهرهای زمانی قابل‌اطمینان برای استفاده هدف ارزیابی باشند. **نکته کاربردی:** توابع هدف ارزیابی نباید اطلاعات قابل‌اطمینانی در رابطه با زمان فعلی هدف ارزیابی ارائه دهد، بلکه زمان و تاریخ توسط سرپرست به‌صورت دستی یا با استفاده از پروتکل NTP server تنظیم می‌گردد.

شماره الزام	نام خانواده	عنصر امنیتی
		نام عنصر: به‌روزرسانی امن ۱ **شماره مؤلفه: ح‌ت-رم-(ت س)۱٫۱ (FPT_TUD_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید برای سرپرستان امنیتی امکان پرس‌وجو نمودن نسخه در حال اجرا و نسخه‌ی اخیراً نصب‌شده‌ی نرم‌افزار/ میان‌افزار هدف ارزیابی را فراهم نماید.
۴۰	به‌روزرسانی امن (FPT_TUD_EXT)	**نکته کاربردی:** ممکن است نسخه در حال اجرا متفاوت از نسخه که اخیراً نصب‌شده باشد. برای مثال، شاید به‌روزرسانی نصب‌شده باشد، اما قبل از اجرایی شدن این نسخه لازم است سیستم مجدداً راه‌اندازی گردد. بنابراین لازم است در پرس‌وجو هر دو نسخه صریحاً نشان داده شود.
۴۱		**نام عنصر: به‌روزرسانی امن ۱**

شماره الزام	نام خانواده	عنصر امنیتی

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

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید امکان به‌روزرسانی [انتخاب: آنلاین، آفلاین] هدف ارزیابی و [انتخاب: پشتیبانی از بررسی خودکار به‌روزرسانی، پشتیبانی از به‌روزرسانی خودکار، هیچ سازوکار به‌روزرسانی دیگر] برای سرپرستان امنیتی فراهم نماید.

نکته کاربردی:

در این الزام «پشتیبانی از بررسی خودکار به‌روزرسانی» و «پشتیبانی از بروز رسانی خودکار» متفاوت است. اولین مورد به هدف ارزیابی اشاره دارد که در دسترس بودن به‌روزرسانی جدید را بررسی و به سرپرست اطلاع می‌دهد (به عنوان نمونه از طریق یک پیام در طول نشست سرپرست، از طریق یک فایل لاگ) اما لازم است سرپرست برای انجام واقعی به‌روزرسانی اقداماتی انجام دهد. اما دومین انتخاب به هدف ارزیابی اشاره دارد که به‌روزرسانی را بررسی و به‌صورت خودکار آن‌ها را نصب می‌نماید.

شماره الزام	نام خانواده	عنصر امنیتی
		نام عنصر: به‌روزرسانی امن ۱
		شماره مؤلفه: ح‌ت-رم-(ت س)۳,۱ (FPT_TUD_EXT.1.3)
		شرح مؤلفه:
۴۲		توابع امنیتی هدف ارزیابی باید پیش از نصب نسخه به‌روزرسانی شده، با استفاده از [انتخاب: سازوکارهای امضای دیجیتال، مقادیر درهم‌سازی منتشرشده] از صحت به‌روزرسانی نرم‌افزار/میان‌افزار اطمینان حاصل نمایند.
		نکته کاربردی:
		سازوکار امضاء دیجیتال در این الزام به الگوریتم مشخص‌شده در FCS_COP.1(2) اشاره دارد.
		درهم‌سازی منتشرشده توسط یکی از توابع مشخص‌شده در الزام FCS_COP.1(3) تولید می‌شود.
		نویسنده هدف امنیتی باید سازوکارهای پیاده‌سازی شده توسط هدف ارزیابی را انتخاب نمایند.

۵,۷ کلاس دسترسی به هدف ارزیابی۱

شماره الزام	نام خانواده	عنصر امنیتی
۴۳	قفل‌کردن و خاتمه دادن نشست (FTA_SSL)	**نام عنصر: قفل نمودن نشست‌های شروع‌شده توسط توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: دس-قن-(ت‌س).۱,۱(FTA_SSL_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پس از غیرفعال بودن نشست برای یک مدت‌زمان مشخص نشست را [انتخاب: • *قفل نماید- غیر فعال‌سازی کلیه فعالیت‌های مربوط به دسترسی داده‌های کاربر و دستگاه‌های نمایش. همچنین لازم است که پیش از باز شدن نشست توابع امنیتی هدف ارزیابی، سرپرست را دوباره احراز هویت نماید.* • *خاتمه دهد*]. مدت‌زمان مشخص غیرفعال بودن، توسط سرپرست تعیین گردد.

1 TOE access(FTA)

شماره الزام	نام خانواده	عنصر امنیتی
۴۴		**نام عنصر: قفل‌گذاری بر روی نشست‌ها و خاتمه دادن به آن‌ها ۳** **شماره مؤلفه: دس-ق‌ن.۱,۳(FTA_SSL.3.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید نشست تعاملی راه دور[1] را پس از مدت‌زمان مشخص غیرفعال بودن، خاتمه دهد. مدت‌زمان مشخص غیرفعال بودن، توسط سرپرست تعیین گردد.
۴۵		**نام عنصر: قفل‌گذاری بر روی نشست‌ها و خاتمه دادن به آن‌ها ۴** **شماره مؤلفه: دس-ق‌ن.۱,۴(FTA_SSL.4.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به شروع‌کننده نشست، اجازه اتمام نشست تعاملی خودش را بدهند.

[1] Remote

۵,۸ کلاس کانال‌ها / مسیرهای مورد اعتماد۱

شماره الزام	نام خانواده	عنصر امنیتی
۴۶	کانال مورد اعتماد بین توابع امنیتی هدف ارزیابی **(FTP_ITC)**	**نام عنصر: کانال مورد اعتماد داخلی توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: مم-ک‌م.۱,۱ (FTP_ITC.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید با استفاده از پروتکل [انتخاب: *IPsec ،SSH ،TLS ،TLS/HTTPS*] کانال ارتباطی قابل‌اطمینانی را میان خود و سایر محصولات فناوری اطلاعات برقرار نماید که از قابلیت سرور ممیزی، [انتخاب: *سرور احراز هویت، [اختصاص: **دیگر ویژگی‌ها***]] پشتیبانی می‌نماید، کانال ارتباطی برقرارشده به‌طور منطقی از سایر کانال‌های ارتباطی جدا است و به‌صورت مطمئن نقطه پایانی‌اش را شناسایی می‌نماید و از داده‌های کانال در برابر تغییر یا افشاء، محافظت می‌کند.

1 Trusted path/channels(FTP)

شماره الزام	نام خانواده	عنصر امنیتی

نام عنصر: کانال مورد اعتماد 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 خود و سایر محصولات فناوری اطلاعات مطمئن بدهند.

۴۷

نکته کاربردی:

منظور از این الزام، استفاده از پروتکل‌های رمزنگاری برای حفاظت ارتباطات هدف ارزیابی با موجودیت‌های IT مجاز است. در این الزام برای ارتباط هدف ارزیابی با سروری که اطلاعات ممیزی را جمع‌آوری می‌نماید، از پروتکل‌های نامبرده شده استفاده می‌گردد.

در صورتی که هدف ارزیابی در ارتباط با یک سرور احراز هویت باشد (به‌طور مثال RADIUS)، نویسنده سند هدف امنیتی در دومین انتخاب، «سرور احراز هویت» را انتخاب می‌نماید و از یکی از پروتکل‌های نامبرده شده در

شماره الزام	نام خانواده	عنصر امنیتی
		الزام برای حفاظت از ارتباط استفاده می‌نماید.
		اگر دیگر موجودیت‌های IT مجاز (همانند NTP Server) دارای ارتباط محافظت‌شده‌ای هستند، نویسنده هدف امنیتی در قسمت «اختصاص»، از آن موجودیت نام می‌برد و در قسمت «انتخاب» پروتکلی را انتخاب می‌نماید که از این ارتباط محافظت می‌نماید.
		پس از آنکه نویسنده هدف امنیتی در اولین «انتخاب»، پروتکل‌های مناسب را انتخاب نمود، از پیوست دو این پروفایل حفاظتی، الزامات مربوط به آن پروتکل را نیز در سند هدف امنیتی می‌آورد.
		نام عنصر: کانال مورد اعتماد داخلی توابع امنیتی هدف ارزیابی ۱
		شماره مؤلفه: مم-ک‌م.۳,۱ (FTP_ITC.1.3)
۴۸		**شرح مؤلفه:**
		توابع امنیتی هدف ارزیابی باید ارتباطات با [اختصاص: **فهرستی از سرویس‌هایی که توابع امنیتی هدف ارزیابی قادر به شروع نمودن ارتباط با آن‌ها هستند**] از طریق کانال مورد اعتمادی شروع نمایند.

شماره الزام	نام خانواده	عنصر امنیتی

نکته کاربردی:

درحالی‌که هیچ الزام دیگری برای شروع ارتباطات وجود ندارد، نویسنده هدف امنیتی در قسمت «اختصاص» سرویس‌هایی را لیست می‌نماید که هدف ارزیابی بتواند ارتباطش را با آن‌ها شروع نماید.

این الزام نشان می‌دهد که ارتباطات نه‌تنها در زمان برقراری ارتباط محافظت می‌گردند، بلکه پس از قطعی، ارتباط محافظت‌شده دوباره از سر گرفته می‌شود. در مواردی که بخشی از تنظیمات هدف ارزیابی، به‌صورت دستی تونل‌ها را جهت حفاظت ارتباطات دیگر تنظیم می‌نماید، چنانچه پس از قطعی ارتباط، هدف ارزیابی سعی در برقراری مجدد ارتباط به‌صورت خودکار یا دستی نماید، ممکن است فرصتی برای مهاجم ایجاد گردد تا به اطلاعات حساس، دسترسی پیدا نماید یا اتصال را به خطر اندازد.

نام عنصر: مسیر مطمئن ۱

۴۹	مسیر مطمئن (**FTP_TRP**)	**شماره مؤلفه: مم-مم.۱،۱ (FTP_TRP.1.1)**

شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی
		توابع امنیتی هدف ارزیابی، باید مسیر ارتباطی امنی با استفاده از [انتخاب: *IPsec ،SSH ،TLS ،TLS/HTTPS*] میان خود و سرپرست از راه دور فراهم نماید که به‌صورت منطقی از دیگر مسیرهای ارتباطی مجزا باشد، هم‌چنین نقاط پایانی[1] خود را به‌صورت مطمئن شناسایی و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات داده‌های تبادلی را تشخیص می‌دهد.
		نام عنصر: مسیر مطمئن ۱
		شماره مؤلفه: مم-مم.۲,۱ (FTP_TRP.1.2)
۵۰		**شرح مؤلفه:**
		توابع امنیتی هدف ارزیابی باید به سرپرست از راه دور، اجازه ایجاد ارتباط از طریق مسیر مطمئن را بدهند.
۵۱		**نام عنصر: مسیر مطمئن ۱**

1End points

شماره الزام	نام خانواده	عنصر امنیتی

شماره مؤلفه: مم-مم.۳,۱.۳ (FTP_TRP.1.3)

شرح مؤلفه:

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

نکته کاربردی:

این الزام اطمینان می‌دهد که سرپرستان از راه دور تمام ارتباطاتشان را با هدف ارزیابی از طریق یک مسیر امن شروع می‌نمایند، و تمام ارتباطات با هدف ارزیابی توسط سرپرستان از راه دور بر روی این مسیر انجام می‌گیرد. داده منتقل‌شده در این کانال ارتباطی امن توسط پروتکلی که در «انتخاب» اول برگزیده‌شده است، رمز می‌گردد. نویسنده هدف امنیتی سازوکار و یا سازوکارهای پشتیبانی شده توسط هدف ارزیابی را انتخاب می‌نماید و این اطمینان را می‌دهد که جزئیات الزامات آمده در پیوست دو را به سند هدف امنیتی اضافه می‌کند.

۵,۹ کلاس هانی پات

شماره الزام	نام خانواده	عنصر امنیتی
۵۲	مجموعه داده‌های سیستم (HONEYPOT_SDC.1.1)	**نام عنصر: مجموعه داده‌های سیستم ۱** **شماره مؤلفه: ت‌ن-دس-(ت‌س).۱,۱ (HONEYPOT_SDC.1.1)** **شرح مؤلفه:** هدف ارزیابی (حس‌گرها) نباید سرویس و اطلاعات واقعی را در مورد دیگر اجزای سیستم و شبکه در اختیار تعامل کننده قرار دهد.
۵۳		**نام عنصر: مجموعه داده‌های سیستم ۱** **شماره مؤلفه: ت‌ن-دس-(ت‌س).۲,۱ (HONEYPOT_SDC.1.2)** **شرح مؤلفه:** سیستم حداقل باید اطلاعات زیر را جمع‌آوری و ثبت کند: • تاریخ و زمان رویداد، نوع رویداد، شناسه موجودیت فعال، و نتایج (موفقیت یا شکست) رویداد

شماره الزام **نام خانواده**

عنصر امنیتی

جزئیات	رویداد	نام مؤلفه
موجودیت[1] سیستم تشخیص نفوذ، دسترسی موردتقاضا، آدرس مبدأ، آدرس مقصد	دستیابی داده	ت‌ن-دس.۱
سرویس مشخص، آدرس مبدأ، آدرس مقصد	درخواست سرویس	ت‌ن-دس.۱
آدرس مبدأ، آدرس مقصد	تغییر دادن تنظیمات امنیتی	ت‌ن-دس.۱
موقعیت، شناسایی کد	* کد مخرب	ت‌ن-دس.۱
شناسایی سرویس(نام یا پورت)، واسطه، پروتکل‌ها	تنظیمات سرویس	ت‌ن-دس.۱

۵۴ واکنش
(HONEYPOT

[1] Object

شماره الزام	نام خانواده	عنصر امنیتی

نام عنصر: واکنش تشخیص نفوذ (RCT_)

شماره مؤلفه: ت‌ن-وا-(ت‌س).۱,۱.۱ (HONEYPOT_RCT.1.1)

شرح مؤلفه:

هدف ارزیابی در زمان تشخیص یک نفوذ، باید یک هشدار به [اختصاص: **مقصد هشدار**] ارسال نماید و [اختصاص: **اقدامات مناسب**] را انجام دهد.

نکته کاربردی:

هدف ارزیابی باید در صورت روی دادن یک نفوذ به مدیر مجاز هشدار دهد.

۶ الزامات تضمین امنیتی

نام کلاس	نام کامپوننت	توضیحات
Development	ADV_FSP.2	مشخصات کارکرد ابتدایی
	ADV_ARC.1	معماری امنیتی
	ADV_TDS.1	طراحی اولیه
Guidance Documents	AGD_OPE.1	راهنمای کاربری

	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.2	آزمون مستقل-منطبق
	ATE_FUN.1	آزمون کارکردی
	ATE_COV.1	پوشش
Vulnerability Assessment	AVA_VAN.2	آنالیز آسیب‌پذیری
Life cycle Support	ALC_CMC.2	استفاده از سیستم پیکربندی
	ALC_CMS.2	پوشش پیکربندی هدف ارزیابی
	ALC_DEL.1	رویه‌ها تحویل
	ALC_CMS.2	رویه‌های گزارش دهی نقص

جدول ۲: الزامات تضمین امنیتی

۶,۱ 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 الزامات کارکردی و مورد تائید توسعه‌دهندگان 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 تهدیداتی است که با محرمانگی و صحت داده‌های کاربری که در میان شبکه منتقل می‌گردند یا داده‌های احراز هویتی که ممکن است پیمایش کننده اتصال باشد، مقابله می‌نمایند (از طریق اتصالات همتا به همتا هدف ارزیابی یا اتصال هدف ارزیابی به VPN Gateway). همچنین

[1] TOE Security Specification

هدف ارزیابی با توجه به پیکربندی‌اش، ممکن است پیشنهاد حفاظت از دسترسی غیرمجاز به شبکه پشت هدف ارزیابی نماید. علاوه بر واسط‌های شبکه لازم است که واسط-های سرپرستی (چگونه هدف ارزیابی پیکربندی می‌شود) شرح داده شود.

۶,۱,۱معماری امنیتی

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱	معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید هدف ارزیابی را طوری پیاده‌سازی و طراحی نماید که نتوان ویژگی‌های امنیتی توابع امنیتی هدف ارزیابی را دور زد.
۲		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.2D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		توسعه‌دهنده باید طوری توابع امنیتی هدف ارزیابی را طراحی و پیاده‌سازی نماید تا بتواند از خود در برابر مداخله توسط موجودیت‌های فعال ناامن، محافظت نماید.
۳		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.3D)** **شرح مؤلفه:** توسعه‌دهنده باید توصیفی از معماری امنیتی توابع امنیتی هدف ارزیابی ارائه نماید.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۴	معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.1C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: سند معماری امنیتی باید سطح جزئیاتش متناسب با توصیف واسط اجراکننده کارکرد امنیتی باشد که در سند طراحی هدف ارزیابی ذکرشده است.
۵		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.2C)** **شرح مؤلفه:** سند معماری امنیتی باید دامنه امنیتی نگهداری شده توسط توابع امنیتی هدف ارزیابی سازگار با الزامات کارکرد امنیتی را توصیف نماید.
۶		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.3C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند معماری امنیتی، باید چگونگی مقداردهی اولیه توابع امنیتی هدف ارزیابی را توصیف نماید.
۷		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.4C)** **شرح مؤلفه:** سند معماری امنیتی باید نشان دهد که توابع امنیتی هدف ارزیابی از خود در برابر مداخله محافظت می‌نماید.
۸		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_ARC.1.5C)** **شرح مؤلفه:** سند معماری امنیتی باید نشان دهد، توابع امنیتی هدف ارزیابی از دور زدن عملکرد واسط اجراکننده کارکرد امنیتی جلوگیری می‌نماید.

مؤلفه‌های اقدامات ارزیاب

شماره الزام	نام خانواده	عنصر امنیتی
۹	معماری امنیتی **(ADV_ARC)**	**نام عنصر: توصیف معماری امنیتی ۱** **شماره مؤلفه: (ADV_ARC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.

۶,۱,۲ مشخصات کارکردی

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

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۰	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (ADV_FSP.2.1D) **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
۱۱		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۲	مشخصات کارکردی	**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
	(ADV_FSP)	**شماره مؤلفه: (ADV_FSP.2.1C)** **شرح مؤلفه:** مشخصات کارکردی باید توابع امنیتی هدف ارزیابی را به‌طور کامل نمایش دهد.
۱۳		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورداستفاده برای تمام واسط‌های توابع امنیتی هدف ارزیابی را توصیف نماید.
۱۴		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.3C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مشخصات کارکردی باید تمام پارامترهای مربوط به هر واسط توابع امنیتی هدف ارزیابی را معرفی و توصیف نماید.
۱۵		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.4C)** **شرح مؤلفه:** برای هر واسط اجراکننده کارکرد امنیتی، مشخصات کارکردی باید اقدامات آن واسط را توصیف نمایند.
۱۶		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.5C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		برای واسط اجراکننده کارکرد امنیتی، سند مشخصات کارکردی باید پیغام خطاهایی را توصیف نماید که مستقیماً از پردازش اقدامات اجراکننده کارکرد امنیتی ناشی شده‌اند.
۱۷		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.6C)** **شرح مؤلفه:** ردیابی‌ها باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌ها در سند مشخصات کارکردی باشند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۸	مشخصات کارکردی	**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
	(ADV_FSP)	**شماره مؤلفه: (ADV_FSP.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
۱۹		**نام عنصر: مشخصات کارکردی واسط اجراکننده کارکرد امنیتی ۲** **شماره مؤلفه: (ADV_FSP.2.2E)** **شرح مؤلفه:** ارزیاب باید مشخص نماید که سند مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

۶,۱,۳ طراحی

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۰	مشخصات کارکردی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید طراحی هدف ارزیابی را ارائه نماید.
۲۱		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید نگاشتی از واسط‌های سند مشخصات کارکردی به پایین‌ترین سطح از اجزاء طراحی هدف ارزیابی ارائه نماید.

مؤلفه‌های محتوایی

شماره الزام	نام خانواده	عنصر امنیتی
۲۲	مشخصات کارکردی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.1C)** **شرح مؤلفه:** طراحی باید ساختار هدف ارزیابی را به‌صورت زیرمجموعه‌ای توصیف نماید.
۲۳		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.2C)** **شرح مؤلفه:** سند طراحی باید تمام زیرمجموعه‌های توابع امنیتی هدف ارزیابی را معرفی نماید.
۲۴		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.3C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند طراحی باید رفتار هر زیرمجموعه پشتیبان کننده‌ی الزام کارکرد امنیتی و غیر مداخله کننده‌ی الزام کارکرد امنیتی را با جزئیات کافی شرح داده تا نشان دهد که زیرمجموعه اجراکننده کارکرد امنیتی نمی‌باشند.
۲۵		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.4C)** **شرح مؤلفه:** طراحی باید به‌طور خلاصه رفتار اجراکننده کارکرد امنیتی از زیرمجموعه‌های اجراکننده کارکرد امنیتی را بیان نماید.
۲۶		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.5C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		طراحی باید شرحی از تعاملات بین زیرمجموعه‌های اجراکننده کارکرد امنیتی و هم‌چنین بین این زیرمجموعه‌ها و دیگر زیرمجموعه‌ها بیان دارد.
۲۷		**نام عنصر: طراحی اولیه ۱** **شماره مؤلفه: (ADV_TDS.1.6C)** **شرح مؤلفه:** نگاشت باید نشان دهد که تمام رفتاری که در سند طراحی توصیف‌شده است به واسطه‌های درخواست‌کننده آن‌ها نگاشت شده‌اند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۸	مشخصات کارکردی **(ADV_TDS)**	**نام عنصر: طراحی اولیه ۱**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (ADV_TDS.1.1E) **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۶,۲ 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 (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

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

- دستورالعمل نصب موفقیت‌آمیز هدف ارزیابی در محیط
- دستورالعمل مدیریت امنیت هدف ارزیابی به عنوان یک محصول یا به عنوان بخشی از یک محیط عملیاتی بزرگ‌تر
- دستورالعمل‌هایی که ارائه‌دهنده قابلیت سرپرستی محافظت‌شده از طریق استفاده از قابلیت‌های هدف ارزیابی، محیط عملیاتی یا هر دو است.

۶,۲,۱ راهنمای کاربردی

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

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۰	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی که باید در یک

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		محیط پردازشی امن کنترل شوند را توصیف نماید، همانند هشدارهای مناسب.
۳۱		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه‌شده توسط هدف ارزیابی به‌صورت امن استفاده می‌گردد.
۳۲		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به‌خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به‌صورت مناسبی تعیین نماید.

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

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

مؤلفه‌های اقدامات ارزیاب

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

۶,۲,۲ راهنمای آماده‌سازی

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

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		توسعه‌دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه نماید.

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

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

مؤلفه‌های اقدامات ارزیاب		
۴۱	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
۴۲		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب		
		ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تائید نماید، هدف ارزیابی می‌تواند به‌صورت امن برای عمل نمودن آماده شود.

۶,۳ 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 بر اساس کارکردی که برای هدف ارزیابی در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار قرار می‌گیرند، انجام می‌گردد. یکی از خروجی‌های اولیه روال ارزیابی گزارش آزمون است که در الزامات زیر مشخص‌شده است.

۶,۳,۱ آزمون پوشش

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۴۳	آزمون پوشش **(ATE_COV)**	**نام عنصر: آزمون پوشش ۱**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (ATE_COV.1.1D) **شرح مؤلفه:** توسعه‌دهنده باید مدارک آزمون پوشش را ارائه نماید.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۴۴	آزمون پوشش **(ATE_COV)**	**نام عنصر: آزمون پوشش ۱** **شماره مؤلفه: (ATE_COV.1.1C)** **شرح مؤلفه:** مدارک ارائه‌شده برای آزمون پوشش باید نشان‌دهنده ارتباط بین آزمون‌های سند آزمون و واسطهای توابع امنیتی هدف ارزیابی در سند مشخصات کارکردی باشند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۴۵	آزمون پوشش **(ATE_COV)**	**نام عنصر: آزمون پوشش ۱** **شماره مؤلفه: (ATE_COV.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۶,۳,۲ آزمون کارکردی

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۴۶	آزمون کارکردی **(ATE_FUN)**	**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		توسعه‌دهنده باید توابع امنیتی هدف ارزیابی را آزمون نماید و نتایج آن را مستند کند.
۴۷		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید سند آزمون را ارائه نماید.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۴۸	آزمون کارکردی **(ATE_FUN)**	**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.1C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند آزمون باید شامل طرح آزمون، نتایج مورد انتظار آزمون و نتایج واقعی آزمون باشد.
۴۹		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.2C)** **شرح مؤلفه:** طرح آزمون باید آزمون‌های صورت گرفته را معرفی و انجام هر آزمون را توصیف نماید. این سناریو همچنین باید شامل ترتیب وابستگی به نتایج دیگر آزمون‌ها باشد.
۵۰		**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.3C)** **شرح مؤلفه:** نتایج آزمون باید نشان‌دهنده خروجی مورد انتظار از موفقیت‌آمیز آزمون باشد.
۵۱		**نام عنصر: آزمون کارکردی ۱**

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (ATE_FUN.1.4C) **شرح مؤلفه:** نتایج واقعی آزمون باید با نتایج مورد انتظار آزمون سازگار باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۲	آزمون کارکردی **(ATE_FUN)**	**نام عنصر: آزمون کارکردی ۱** **شماره مؤلفه: (ATE_FUN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.

۶,۳,۳ آزمون مستقل

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

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۳	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمون نمودن، هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۴	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل 2** **شماره مؤلفه: (ATE_IND.2.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمون نمودن باشد.
۵۵		**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.2C)** **شرح مؤلفه:** توسعه‌دهنده باید معادل مجموعه منابعی که در آزمون کارکردی توسعه‌دهنده استفاده‌شده‌اند برای ارزیاب فراهم نماید.

مؤلفه‌های اقدامات ارزیاب		
۵۶	آزمون مستقل	**نام عنصر: آزمون مستقل ۲**

مؤلفه‌های اقدامات ارزیاب		
	(ATE_IND)	**شماره مؤلفه: (ATE_IND.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
۵۷		**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.2E)** **شرح مؤلفه:** ارزیاب باید نمونه‌ای از آزمون‌ها در سند آزمون را اجرا نماید تا از نتایج آزمون توسعه‌دهنده اطمینان حاصل نماید.
۵۸		**نام عنصر: آزمون مستقل ۲** **شماره مؤلفه: (ATE_IND.2.3E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را آزمون نماید تا اطمینان حاصل نماید که توابع

مؤلفه‌های اقدامات ارزیاب		
		امنیتی هدف ارزیابی به‌صورت مشخص‌شده عمل می‌نماید.

۶,۴ کلاس آسیب‌پذیری

برای آماده نمودن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی آن دسته از آسیب‌پذیری‌هایی که در این نوع محصولات یافت شده-اند بیابد. در اغلب مواقع سوءاستفاده از این آسیب‌پذیری‌ها (یافتن آسیب‌پذیری‌های در آزمایشگاه) نیاز به مهارت و تخصص مهاجمان دارد.

تا زمانی که ابزارهای نفوذ در تمام آزمایشگاه‌ها توزیع می‌شوند و در دسترس هستند، انتظار نمی‌رود که ارزیاب‌ها برای این دسته از آسیب‌پذیری‌ها 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 گردد. این‌گونه اطلاعات در توسعه ابزارهای آزمون نفوذ و همچنین نسخه‌های بعدی پروفایل‌های حفاظتی مورداستفاده قرار خواهند گرفت.

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۵۹	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.1D)**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شرح مؤلفه: توسعه‌دهنده باید برای آزمون نمودن، هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۶۰	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمون نمودن باشد.

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

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۶۱	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
۶۲		**نام عنصر: آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد.
۶۳		**نام عنصر: آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.3E)**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: ارزیاب باید آنالیز آسیب‌پذیری هدف ارزیابی را با استفاده از مستندات راهنما، سند مشخصات کارکردی، طراحی هدف ارزیابی و توصیف معماری امنیتی انجام دهد تا آسیب‌پذیری‌های بالقوه در هدف ارزیابی را معرفی نماید.
۶۴		**نام عنصر: آسیب‌پذیری ۲** **شماره مؤلفه: (AVA_VAN.2.4E)** **شرح مؤلفه:** ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ را انجام دهد تا مقاومت هدف ارزیابی در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۶,۵ کلاس پشتیبانی از چرخه حیات

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

۶,۵,۱ قابلیت‌های پیکربندی

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

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۶۵	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.1D)**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: توسعه‌دهنده باید هدف ارزیابی و مرجع هدف ارزیابی را ارائه نماید.
۶۶		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.2D)** **شرح مؤلفه:** توسعه‌دهنده باید سند پیکربندی را ارائه نماید.
۶۷		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.3D)** **شرح مؤلفه:** توسعه‌دهنده باید از یک سیستم پیکربندی استفاده نماید.

مؤلفه‌های اقدامات محتوایی

شماره الزام	نام خانواده	عنصر امنیتی
۶۸	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.1C)** **شرح مؤلفه:** هدف ارزیابی باید با یک مرجع یکتا برچسب زده شود.
۶۹		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.2C)** **شرح مؤلفه:** مستندات پیکربندی باید روش مورداستفاده برای معرفی یکتای موارد پیکربندی را معرفی نماید.
۷۰		**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.3C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		سیستم پیکربندی باید تمام موارد پیکربندی را به‌صورت یکتا معرفی نماید.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۱	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: استفاده از یک سیستم پیکربندی۲** **شماره مؤلفه: (ALC_CMC.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۶,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۲	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۳	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود هدف ارزیابی، مدارک موردنیاز توسط الزامات تضمین امنیتی و بخش-هایی که شامل هدف ارزیابی هستند، باشد.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۷۴		**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.2C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به‌صورت یکتا معرفی نماید.
۷۵		**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۲** **شماره مؤلفه: (ALC_CMS.2.3C)** **شرح مؤلفه:** برای هر یک از موارد پیکربندی مربوط به توابع امنیتی هدف ارزیابی، لیست پیکربندی باید توسعه‌دهنده آن را نشان دهد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۶	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷۷	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی بخشی از هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۶,۵,۳ تحویل

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۷۸	تحویل (ALC_DEL)	**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید رویه تحویل هدف ارزیابی یا بخشی از آن را به مشتری، مستند نماید.
۷۹		**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید از رویه‌های تحویل استفاده نمایند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۸۰	تحویل **(ALC_DEL)**	**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.1C)** **شرح مؤلفه:** مستندات تحویل باید تمام رویه‌هایی که برای حفظ امنیت در زمان توزیع نسخه‌های هدف ارزیابی لازم و ضروری هستند را شرح دهد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۸۱	تحویل **(ALC_DEL)**	**نام عنصر: رویه تحویل ۱** **شماره مؤلفه: (ALC_DEL.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نمایند.

۶,۵,۴ اصلاح نقص

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۸۲	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.1D)** **شرح مؤلفه:** توسعه‌دهنده باید رویه‌های اصلاح نقص که به توسعه‌دهنده هدف ارزیابی داده می‌شوند را مستند نماید.
۸۳		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.2D)** **شرح مؤلفه:** توسعه‌دهنده باید رویه‌ای برای پذیرش تمام گزارش‌های نقص امنیتی و اقدام نمودن بر روی آن‌ها، هم-چنین درخواست تصحیح نقص ایجاد نماید.

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۸۴		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.3D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای اصلاح نقص را به کاربران هدف ارزیابی ارائه نماید.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۸۵	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.1C)** **شرح مؤلفه:** مستندات رویه‌های اصلاح نقص باید رویه‌هایی را توصیف نمایند که در هر هدف ارزیابی منتشرشده برای پیگیری نقص‌های امنیتی گزارش‌شده مورداستفاده قرار می‌گیرند.

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۸۶		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.2C)** **شرح مؤلفه:** رویه‌های اصلاح نقص باید ملزم به توصیف ماهیت و اثر هر نقص امنیتی ارائه‌شده، هم‌چنین وضعیت اصلاحیه یافته شده برای آن نقض باشند.
۸۷		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.3C)** **شرح مؤلفه:** رویه‌های اصلاح نقص باید ملزم به معرفی اقدامات اصلاحی برای هر نقض امنیتی باشند.
۸۸		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.4C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مستندات رویه‌های اصلاح نقص باید متدهایی را توصیف نمایند که به کاربران هدف ارزیابی، اطلاعات نقص، اصلاحیه‌ها و راهنمایی در رابطه با اقدامات اصلاحی ارائه می‌دهند.
۸۹		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.5C)** **شرح مؤلفه:** رویه‌های اصلاح نقص باید امکانی را فراهم نمایند تا توسعه‌دهنده بتواند گزارش‌های و درخواست‌های مربوط به نقص‌های امنیتی مشکوک در هدف ارزیابی را از کاربران آن دریافت نماید.
۹۰		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.6C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		رویه‌ی پردازش نقص امنیتی گزارش‌شده، باید اطمینان دهد که هر نقص گزارش‌شده اصلاح می‌گردد و هم‌چنین رویه اصلاح به کاربر هدف ارزیابی داده می‌شود.
۹۱		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.7C)** **شرح مؤلفه:** رویه پردازش نقص امنیتی گزارش‌شده، باید هرگونه اصلاح نقص امنیتی را از مطرح نمودن نقص جدید در هدف ارزیابی حفاظت نماید.
۹۲		**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.8C)** **شرح مؤلفه:** راهنمای اصلاح نقص باید امکانی را فراهم نماید که کاربران هدف ارزیابی بتوانند هرگونه نقص امنیتی

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		مشکوک در هدف ارزیابی را به توسعه‌دهنده گزارش دهند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۹۳	اصلاح نقص **(ALC_FLR)**	**نام عنصر: رویه گزارش نقص ۲** **شماره مؤلفه: (ALC_FLR.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نمایند.

پیوست یک: فرهنگ اصطلاحات

- **استاندارد ارزیابی معیار مشترک (CC)**

استاندارد ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

- **متدولوژی ارزیابی معیار مشترک[1] (CEM)**

متدلوژی ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

- **هدف ارزیابی (TOE)**

محصول مورد ارزیابی؛ که در این سند، هانی پات با تعامل کم است.

- **غیر هدف ارزیابی (Non-TOE[2])**

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

- **محیط عملیاتی (Operational Environment)**

محیطی که هدف ارزیابی در آن عمل می‌کند.

- **پروفایل حفاظتی (PP[1])**

[1] Common Evaluation Methodology(CEM)

[2] Non-Target Of Evaluation

مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات؛ مجموعه‌ای که مستقل از پیاده‌سازی است.

- **هدف امنیتی (ST[2])**

مجموعه‌ای از الزامات امنیتی برای یک محصول خاص؛ مجموعه‌ای که وابسته به پیاده‌سازی است.

- **مسائل امنیتی (Security Problem)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «مشکل امنیتی» وجود دارد که به‌طور رسمی ماهیت و حوزه امنیت در نظر گرفته‌شده توسط هدف ارزیابی را تعریف می‌نماید.

این بیانیه شامل موارد زیر است:

–«تهدیداتی» 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)**

موجودیت‌هایی که می‌توانند بر روی دارایی‌ها اقدام تهاجمی انجام دهند.

- **خط‌مشی امنیتی سازمانی (OSP[3])**

[1] Protection Profile

[2] Security Target

[3] Organizational Security Policy

مجموعه‌ای از قوانین، که توصیف‌کننده رفتار امنیتی خاصی است که توسط «توابع امنیتی هدف ارزیابی» اجرا می‌گردند؛ این مجموعه قوانین به‌صورت یک مجموعه از «الزام‌های کارکرد امنیتی» قابل‌بیان است.

- **اهداف امنیتی (Security Objective)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «اهداف امنیتی» وجود دارد که برای مقابله با تهدیدات معرفی‌شده و/یا برای برآورده نمودن خط‌مشی‌های امنیت سازمان و یا فرضیات معرفی‌شده در بخش «مسائل امنیتی»، در نظر گرفته‌شده است.

- **الزام امنیتی (Security Requirement)**

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

- **الزام کارکرد امنیتی(SFR[1])**

الزامات اجرای امنیت توسط هدف ارزیابی.

- **الزامات تضمین امنیتی (SAR[2])**

الزامات تضمین امنیت هدف ارزیابی.

- **بسته (Package)**

نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی است. 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» برگرفته‌شده است، و نشان‌دهنده سطح امنیتی محصول است. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» است.

- **خلاصه مشخصه هدف ارزیابی[2] (TSS)**

شرحی از این‌که یک هدف ارزیابی چگونه الزامات کارکرد امنیتی را در یک هدف امنیتی برآورده می‌سازد.

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

عملکرد امنیتی محصول مورد ارزیابی.

- **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 استفاده‌شده توسط توابع امنیتی هدف ارزیابی هستند.

- **داده کاربری (User data)**

[1] Evaluation Assurance Level

[2] TOE Summary Specification (TSS)

[3] TOE Security Functions (TSF)

داده‌های کاربری هستند که عملکرد توابع امنیتی هدف ارزیابی را تحت تأثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره‌شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به‌کاربرده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری است.

- **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 تأکید، تفاوت دارند.

- **عنصر (Component)[۱]**

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

- **مؤلفه (Element)[۲]**

بیانی از نیاز امنیتی که غیرقابل تجزیه است.

- **الزام (Assignment)**

مشخص نمودن پارامترهای معرفی‌شده در یک مؤلفه (از استاندارد معیار مشترک) یا الزام است.

- **انتخاب (Selection)**

[۱] در استاندارد ISO 14508 منتشر شده توسط سازمان استاندارد، Component مولفه ترجمه شده است.

[۲] در استاندارد ISO 14508 منتشر شده توسط سازمان استاندارد، Element عنصر ترجمه شده است.

انتخاب نمودن یک یا بیش از یک آیتم در فهرستی که در مؤلفه یا الزام وجود دارد.

- **سرپرست (Administrator)**

موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی هدف ارزیابی بر عهده دارد و معمولاً 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. به‌عبارت‌دیگر 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 می‌نماید، و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره. به‌عبارت‌دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله‌کننده، 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، مورداستفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند همچون نام فایل که ممکن است

برای معرفی منابع منحصربه‌فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به‌طور خاص برای اجراشدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به‌طورکلی «مشخصه امنیتی» نامیده می‌شود.

- **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 «خط‌مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که هدف ارزیابی باید اجرا نماید، تعریف کند. هرکدام 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 «خط‌مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» سازوکارهایی هستند که بر اساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، TSF status data و عملکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

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

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

«خط‌مشی جریان اطلاعات» سازوکارهایی هستند که بر اساس 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.

[1] Security Functionality Policy

- **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 استفاده‌شده 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 ذخیره‌شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به‌کاربرده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری است.

پیوست دو: الزامات پروتکل‌های ارتباطی امن

همان‌گونه که در این پروفایل حفاظتی نشان داده‌شده است، چندین روش وجود دارد که هدف ارزیابی منطبق بر این پروفایل حفاظتی، می‌تواند تهدیدات مرتبط با به خطر افتادن کانال ارتباطی بین سرپرستان و دیگر بخش‌های هدف ارزیابی یا موجودیت‌های IT خارجی را کاهش دهد. برای حفاظت از اتصال سرور ممیزی و سرپرستان راه دور باید از یکی از پروتکل‌های ارتباطی امن (IPSEC، SSH، TLS، TLS/HTTPS) استفاده نمود.

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

نویسنده هدف امنیتی باید با توجه به پروتکل‌هایی که در الزامات انتخاب نموده است، الزام مربوط به آن پروتکل را نیز در سند هدف امنیتی کپی نماید. علاوه بر این، با توجه به الزامات انتخاب‌شده، لازم است اطلاعات مناسبی توسط بخش ۸,۲ رویدادهای قابل ممیزی به جدول رویدادهای قابل ممیزی در هدف امنیتی اضافه گردد.

الف: الزامات کارکرد امنیتی

شماره الزام	نام خانواده	عنصر امنیتی
۵۵	رز-اپ-(ت‌س)	نام عنصر: پروتکل IPSEC ۱

شماره الزام	نام خانواده	عنصر امنیتی
FCS_IPSEC_EXT.1 Explicit: IPSEC		شماره مؤلفه: رز-IPSEC-(ت‌س).۱,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید ESP[1]پروتکل IPsec را به‌صورت تعریف‌شده توسط RFC4303 و با استفاده از الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-256 (این دو الگوریتم در RFC 3602 مشخص‌شده‌اند)، [انتخاب: *هیچ الگوریتم دیگر*، *AES-GCM-128*، *AES-GCM-256 مشخص‌شده در RFC 4106*]، و با استفاده از [انتخاب، حداقل یکی از موارد: پروتکل *IKE[2]v1 به‌صورت تعریف‌شده در RFC های2407، 2408، 2409، 4109، و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]*؛ پروتکل *IKEv2 تعریف‌شده درRFC های 5996 ، 4307، و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی*]] پیاده‌سازی نمایند.

نکته کاربردی:

[1] Encapsulating Security Payload

[2] Internet Key Exchange

شماره الزام	نام خانواده	عنصر امنیتی
		در اولین انتخاب می‌توان الگوریتم‌های رمزنگاری بیشتری را برگزید. در دومین انتخاب باید مشخص گردد که از پروتکل IKEv1 پشتیبانی می‌گردد یا IKEv2 برای پروتکل IKEv1، در صورتی که پیاده‌سازی IKE مطابق با RFC 2409 باشد و اضافات و تغییرات در RFC 4109 توصیف‌شده باشد الزام تفسیر می‌گردد. RFC 4868 توابع درهم‌سازی بیشتری را برای استفاده IKEv1 و IKEv2 معرفی می‌نماید.
		نام عنصر: پروتکل IPSEC ۱ **شماره مؤلفه: رز-IPSEC-(ت‌س).۲,۱**
۵۶		**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید این اطمینان را بدهند که تبادلات فاز ۱ IKEv1 تنها در مود اصلی استفاده می‌گردد.
۵۷		**نام عنصر: پروتکل IPSEC ۱** **شماره مؤلفه: رز-IPSEC-(ت‌س).۳,۱**

شماره الزام	نام خانواده	عنصر امنیتی

شرح مؤلفه:
توابع امنیتی هدف ارزیابی باید اطمینان دهد که طول عمر SA مربوط به IKEv1 قادر است برای فاز ۱ SA به ۲۴ ساعت محدود گردد و برای فاز ۲ SA به ۸ ساعت محدود گردد.

نکته کاربردی:
الزام بالا می‌تواند توسط طول عمری که توسط سرپرست امنیتی قابل تنظیم است (با الزامات کلاس مدیریت مناسب، یا دستورات ذکرشده در سندی که در AGD_OPE مطرح‌شده است) انجام شود و یا توسط«کد نویسی سخت» که پیاده‌سازی را محدود می‌نماید.

نام عنصر: پروتکل IPSEC ۱

شماره مؤلفه: رز-IPSEC-(ت‌س).۴,۱

۵۸

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

شماره الزام	نام خانواده	عنصر امنیتی

نکته کاربردی:

الزام بالا می‌تواند توسط طول عمری که توسط سرپرست امنیتی قابل تنظیم است (با الزامات FMT مناسب، یا دستورات ذکرشده در سندی که در AGD_OPE مطرح‌شده است) انجام شود و یا توسط «کد نویسی سخت» که پیاده‌سازی را محدود می‌نماید. نویسنده هدف امنیتی، مقدار عددی را در بازه‌ی مشخص‌شده تعیین می‌نماید.

به‌طورکلی، دستورالعمل‌ها برای تنظیم پارامترهای پیاده‌سازی، همچون طول عمر SA، باید توسط الزامات کلاس مدیریت مشخص گردند و در راهنماهای سرپرستی که برای الزام AGD_OPE تولیدشده، نیز ذکرشده باشند.

نام عنصر: پروتکل IPSEC ۱

۵۹ **شماره مؤلفه: رز-IPSEC-(ت‌س).۵,۱**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE گروه‌های DH، ۱۴(۲۰۴۸ بیت

شماره الزام	نام خانواده	عنصر امنیتی

MODP)، و [انتخاب: ۲۴(۲۰۴۸ بیت MODP)، ۱۹ (۲۵۶ بیت POS)، ۲۰ (۲۵۶ بیت تصادفی ECP)، ۲۱ (۳۸۴ بیت تصادفی ECP)، [اختصاص: ***دیگر گروه‌های DH که توسط هدف ارزیابی پیاده‌سازی شده‌اند***]، هیچ گروه دیگر DH] را پیاده‌سازی می‌نمایند.

نکته کاربردی:

این مؤلفه، هدف ارزیابی را ملزم به پشتیبانی از گروه DH 14 می‌نماید. در صورت پشتیبانی از دیگر گروه‌ها، این گروه‌ها باید انتخاب گردند یا در قسمت «اختصاص» بالا مشخص گردند، در غیر این صورت «هیچ گروه دیگر DH» انتخاب می‌گردد. این الزام به تبادلات IKEv1و (در صورت پیاده‌سازی شدن) به IKEv2 اعمال می‌گردد.

نام عنصر: پروتکل IPSEC ۱

۶۰	**شماره مؤلفه: رز-IPSEC-(ت‌س).۶,۱**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE با استفاده از الگوریتم [انتخاب:

شماره الزام	نام خانواده	عنصر امنیتی
		ECDSA ،rDSA ،DSA] احراز هویت همتا را پیاده‌سازی می‌نمایند.
		نکته کاربردی:
		الگوریتم انتخاب‌شده باید با انتخاب صورت گرفته در مؤلفه FCS_COP.1(2) در ارتباط باشد.
		نام عنصر: پروتکل IPSEC ۱
		شماره مؤلفه: رز-IPSEC-(ت‌س).۷,۱
۶۱		**شرح مؤلفه:**
		توابع امنیتی هدف ارزیابی باید استفاده‌ی کلیدهای از قبل به اشتراک گذاشته‌شده را (همان‌طور که در RFC ها اشاره‌شده است) برای استفاده در احراز هویت نمودن اتصالات خود IPsec پشتیبانی نمایند.
		نام عنصر: پروتکل IPSEC ۱
۶۲		**شماره مؤلفه: رز-IPSEC-(ت‌س).۸,۱**
		شرح مؤلفه:

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید موارد زیر را پشتیبانی نمایند:

کلیدهای از پیش به اشتراک گذارده شده، باید قادر باشند از هر ترکیبی از حروف بزرگ، حروف کوچک، اعداد و کاراکترهای خاص: [انتخاب: *"!"، "@"، "#"، "$"،"٪"،"^"،"&"،"*"،")"،"("، [اختصاص: **دیگر کاراکترها***]] تشکیل گردند.

کلیدهای از پیش به اشتراک گذاشته‌شده ۲۲ کاراکتر و [انتخاب: *[اختصاص: **دیگر طول کلیدهایی که پشتیبانی می‌شود***]، *بدون دیگر اندازه‌های کلید*] باشند.

نکته کاربردی:

نویسنده هدف امنیتی باید کاراکترهای خاصی را انتخاب نماید که توسط هدف ارزیابی قابل پشتیبانی باشد. ممکن است با استفاده از قابلیتی که در قسمت «اختصاص» ارائه‌شده، این اختیار به نویسنده داده‌شده است تا بتواند کاراکترهای بیشتری را تعریف نماید.

برای طول کلیدهای از پیش به اشتراک گذاشته‌شده، طول کلید معمولی (۲۲ کاراکتر) برای کمک به ترویج قابلیت همکاری نیاز است. اگر طول کلیدهای دیگر پشتیبانی می‌شود باید در قسمت «اختصاص»

شماره الزام	نام خانواده	عنصر امنیتی
		لیست گردد، هم‌چنین در این قسمت می‌توان یک محدوده را برای طول کلید مشخص نمود(به‌طور مثال طول کلید از ۵ تا ۵۵ کاراکتر).
		نام عنصر: پروتکل TLS ۱
		شماره مؤلفه: رز-TLS-(ت‌س).۱,۱
		شرح مؤلفه:
۶۳	**رز-ل‌ا-(ت‌س).۱ FCS_TLS_EXT.1 Explicit: TLS**	توابع امنیتی هدف ارزیابی باید یک یا بیش از یکی از پروتکل‌های زیر را [انتخاب: *TLS 1.0 (RFC 2246)*، *TLS 1.1 (RFC 4364)*، *TLS 1.2 (RFC 5264)*]که از دنباله‌های رمز زیر پشتیبانی می‌نمایند پیاده‌سازی نمایند:
		دنباله رمز الزامی:
		TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA

شماره الزام	نام خانواده	عنصر امنیتی

دنباله رمز اختیاری:

[انتخاب:

هیچ‌کدام

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

نکته کاربردی:

در این الزام، نویسنده هدف امنیتی باید پروتکل TLS و دنباله‌های رمز مناسبی را انتخاب نماید. هم-چنین باید با ارائه جزئیات، انطباق پروتکل پیاده‌سازی شده را با استانداردهای معرفی‌شده نشان بدهند.

شماره الزام	نام خانواده	عنصر امنیتی
		می‌توان برای ارائه جزئیات بیشتر، به این عنصر، مؤلفه‌هایی اضافه نمود یا جزئیات بیشتر را در بخش خلاصه مشخصات هدف ارزیابی در سند هدف امنیتی آورد. در پیکربندی‌های ارزیابی‌شده از دنباله رمزهایی استفاده می‌شود که توسط این الزام محدودشده‌اند. در صورتی که در هدف ارزیابی از دنباله‌های رمز اختیاری استفاده می‌شود، نویسنده هدف امنیتی باید آن‌ها را در این الزام انتخاب نماید؛ اگر به غیر از دنباله‌های اجباری، دنباله رمزی جهت پشتیبانی وجود نداشته باشد، «هیچ‌کدام» باید انتخاب گردد. **نام عنصر: پروتکل SSH ۱** **شماره مؤلفه: رز-SSH-(ت‌س).۱,۱**
۶۴	**رز-پ‌ا-(ت‌س).۱** **FCS_SSH_EXT.1** **Explicit: SSH**	**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پروتکل SSH را منطبق بر RFC 4251، 4252، 4253 و 4254 پیاده-سازی نمایند. **نکته کاربردی:**

شماره الزام	نام خانواده	عنصر امنیتی
		نویسنده هدف امنیتی باید با ارائه جزئیات، انطباق پروتکل پیاده‌سازی شده را با استانداردهای معرفی‌شده نشان بدهند. می‌توان برای ارائه جزئیات بیشتر، به این عنصر، مؤلفه‌هایی اضافه نمود یا جزئیات بیشتر را در بخش خلاصه مشخصات هدف ارزیابی در سند هدف امنیتی آورد.
		نام عنصر: پروتکل SSH ۱
		شماره مؤلفه: رز-SSH-(ت‌س).۲,۱
۶۵		**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اطمینان دهند که پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر را که در RFC 4253 توصیف‌شده است پشتیبانی می‌نماید: مبتنی بر کلید عمومی، مبتنی بر کلمه عبور.
		نام عنصر: پروتکل SSH ۱
۶۶		**شماره مؤلفه: رز-SSH-(ت‌س).۳,۱**
		شرح مؤلفه: توابع امنیتی هدف ارزیابی باید اطمینان دهند، همان‌طور که در RFC 4253 توصیف‌شده است، بسته-

شماره الزام	نام خانواده	عنصر امنیتی

های بزرگ‌تر از [اختصاص: **عددی برای مشخص نمودن بایت**] بایت در اتصال انتقال SSH حذف می‌گردند.

نکته کاربردی:

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

نام عنصر: پروتکل SSH ۱

شماره مؤلفه: رز-SSH-(ت‌س).۴,۱

۶۷ **شرح مؤلفه:**

توابع امنیتی هدف ارزیابی باید اطمینان دهند، پیاده‌سازی انتقال SSHاز الگوریتم‌های رمزنگاری زیر استفاده می‌نماید: AES-CBC-128، AES-CBC-256، [انتخاب: *AEAD_AES_128_GCM*، *AEAD_AES_256_GCM*، *بدون هیچ الگوریتم دیگر*].

نکته کاربردی:

شماره الزام	نام خانواده	عنصر امنیتی
		در قسمت «اختصاص» نویسنده هدف امنیتی می‌تواند الگوریتم‌های AES-GCM را انتخاب نماید یا در صورتی که از الگوریتم AES-GCMپشتیبانی نمی‌نماید، «بدون هیچ الگوریتم دیگر» انتخاب می‌گردد. در صورت انتخاب الگوریتم AES-GCMباید نویسنده سند هدف امنیتی، خانواده FCS-COP از کلاس پشتیبانی از رمزنگاری را برای این الگوریتم بیاورد.
		نام عنصر: پروتکل SSH ۱
		شماره مؤلفه: رز-SSH-(ت‌س).۵,۱
۶۸		**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اطمینان دهند، پیاده‌سازی انتقال SSH از الگوریتم‌های کلید عمومی زیر استفاده می‌نماید: SSH_RSA، [انتخاب: *PGP-Sign-RSA*، *PGP-Sign-RSA* ، *بدون هیچ الگوریتم دیگر*].
		نکته کاربردی: استاندارد RFC 4253 الگوریتم‌های کلید عمومی مجاز و ضروری را مشخص کرده است. این الزام سبب

شماره الزام	نام خانواده	عنصر امنیتی
		ضروری شدن SSH-RSAمی‌گردد اما می‌توان در صورت پشتیبانی شدن از PGP-Sign-RSA، PGP-Sign-RS، نویسنده هدف امنیتی آن‌ها را انتخاب نماید. در صورتی که تنها SSH_RSA پیاده‌سازی شده باشد نویسنده در قسمت انتخاب، «بدون هیچ الگوریتم عمومی» را انتخاب می‌نماید.
		نام عنصر: پروتکل SSH ۱
		شماره مؤلفه: رز-SSH-(ت‌س).۶,۱
۶۹		**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اطمینان دهند، الگوریتم‌های صحت داده در اتصال انتقال SSH که یک [انتخاب: *hmac-sha1*، *hmac-sha1-96*، *hmac-md5*، *hmac-md5-96*] است استفاده می‌گردند.
		نام عنصر: پروتکل SSH ۱
۷۰		**شماره مؤلفه: رز-SSH-(ت‌س).۷,۱**
		شرح مؤلفه: توابع امنیتی هدف ارزیابی باید اطمینان دهند، که diffie-hellman-group14-sha1 تنها به روش‌های

شماره الزام	نام خانواده	عنصر امنیتی
		تبادل کلید اجازه می‌دهند تا برای پروتکل SSH استفاده گردند.

شماره الزام	نام خانواده	عنصر امنیتی
		نام عنصر: پروتکل HTTPS ۱
		شماره مؤلفه: رز-HTTPS-(ت‌س).۱,۱
		شرح مؤلفه:
۷۱	**رز-اف-(ت‌س).۱ FCS_HTTPS_EXT.1 Explicit: HTTPS**	توابع امنیتی هدف ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 پیاده‌سازی نمایند.
		نکته کاربردی: نویسنده هدف امنیتی باید با ارائه جزئیات، انطباق پیاده‌سازی پروتکل با استاندارد معرفی‌شده را نشان بدهد. برای ارائه جزئیات می‌توان، مؤلفه‌هایی به این عنصر اضافه نمود یا جزئیات بیشتری را در بخش خلاصه مشخصات هدف ارزیابی سند هدف امنیتی آورد.
۷۲		**نام عنصر: پروتکل HTTPS ۱**

شماره الزام	نام خانواده	عنصر امنیتی

شماره مؤلفه: رز-HTTPS-(ت‌س).۲,۱

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید HTTPS را با استفاده از TLS به‌صورت مشخص‌شده در FCS-TLS-EXT) پیاده‌سازی نمایند.

شماره الزام	نام خانواده	عنصر امنیتی

نام عنصر: انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی ۱

شماره مؤلفه: حت-اد-(ت‌س).۱,۱

حت-اد (FPT-ITT)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید زمانی که داده‌ها بین بخش‌های مجزای هدف ارزیابی از طریق استفاده از پروتکل [انتخاب حداقل یکی از: *IPsec، SSH، TLS، TLS/HTTPS*] انتقال می‌یابند، داده‌ها را از افشاء محافظت نمایند و تغییراتش را تشخیص دهند.

شماره الزام	نام خانواده	عنصر امنیتی

نکته کاربردی:

این الزام اطمینان می‌دهد که تمام ارتباطات بین عناصر هدف ارزیابی توسعه‌یافته، با استفاده از یک کانال ارتباطی رمز شده محافظت می‌گردد. داده‌های منتقل‌شده در این کانال ارتباطی، توسط پروتکلی که در انتخاب اول مشخص‌شده است، رمز می‌گردد. نویسنده هدف امنیتی سازوکار یا سازوکارهایی را انتخاب می‌نماید که توسط هدف ارزیابی پشتیبانی گردد و این اطمینان را می‌دهد که جزئیات الزام در این پیوست، مربوط به انتخابی که نموده‌اند (توسط نویسنده هدف امنیتی) در صورتی که در سند هدف امنیتی وجود نداشته باشد، کپی می‌گردند.

ب: رویداد قابل ممیزی

نویسنده سند هدف امنیتی با توجه به الزاماتی که از قسمت الف این پیوست انتخاب نموده از جدول زیر رویدادهای قابل ممیزی مناسبی را در نظر می‌گیرد:

الزام	رویدادهای قابل ممیزی	محتوای رکورد ممیزی اضافی
FCS_IPSEC_EXT.1	خرابی در ایجاد SA مربوط به IPsec	علت خرابی
FCS_TLS_EXT. 1	ایجاد و خاتمه دادن SA مربوط به IPsec خرابی در ایجاد یک نشست TLS ایجاد و خاتمه دادن نشست TLS	نقطه پایانی اتصال غیر-هدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی علت خرابی نقطه پایانی اتصال غیر-هدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی
FCS_SSH_EXT.1	خرابی در ایجاد یک نشست SSH	علت خرابی
FCS_HTTPS_EXT.1	ایجاد و خاتمه دادن نشست SSH خرابی در ایجاد نشست HTTPS	نقطه پایانی اتصال غیر-هدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی علت خرابی
FCS_ITT.1(1)	ایجاد و خاتمه دادن نشست HTTPS هیچ‌کدام	نقطه پایانی اتصال غیر-هدف ارزیابی (آدرس IP) در هر دو حالت موفق بودن و خرابی

الزام	رویدادهای قابل ممیزی	محتوای رکورد ممیزی اضافی
		هیچ‌کدام
FCS_ITT.1(2)	هیچ‌کدام	هیچ‌کدام