به‌نام خدا

نام گزارش

پروفایل حفاظتی مشترک افزاره شبکه: بسته الحاقی برای کنترل‌کننده محدوده نشست

خرداد ۹۵

نسخه ۱,۰

فهرست

۱- مقدمه

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 ارائه‌شده‌اند، در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

این بسته الحاقی[۱] (EP)، الزامات امنیتی کنترل‌کننده محدوده نشست[۲] (SBC) و نیز مجموعه‌ای از حداقل الزامات پایه موردنظر جهت کاهش تهدیدات تعریف‌شده را فراهم می‌آورد. این بسته الحاقی، به‌خودی‌خود کامل نیست، بلکه با الزامات امنیتی پروفایل حفاظتی مشترک افزاره‌های شبکه[۳] (NDcPP) توسعه می‌یابد. از آنجا که این پروفایل حفاظتی برای کنترل‌کننده‌های محدوده نشست (SBC) اختصاص‌یافته است، محصول[۴] (TOE)، کنترل‌کننده محدوده نشست (SBC) است. در این سند کنترل‌کننده محدوده نشست (SBC) و محصول به‌جای یکدیگر استفاده می‌شوند.

به‌عنوان بسته الحاقی به پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) انتظار می‌رود، محتوای هردوی آن‌ها به شکل مناسبی در زمینه هر هدف امنیتی خاص محصول با هم ترکیب شوند. این بسته الحاقی به‌طور خاص، برای تعریف یک محصول تعریف‌شده است که ممکن است شامل الزامات کارکرد امنیتی این بسته الحاقی و پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) بدون تناقض و ابهام باشد. هدف امنیتی باید نسخه‌های کاربردپذیر پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) و این بسته الحاقی را در ادعای انطباق خود مشخص کند (نسخه جاری را در سایت http://www.niap-ccevs.org/pp/ ببینید).

---

[۱] Extended Package

[۲] Session Border Controller

[۳] Network Devices collaborative Protection Profile

[۴] Target of Evaluation

۲- شرح محصول

۲-۱- محصول منطبق

این بسته الحاقی به‌طور خاص کنترل‌کننده‌های محدوده نشستی (SBC) را موردتوجه قرار می‌دهد که قابلیت ایجاد دیواره آتش، قابلیت تبادل و استفاده از اطلاعات[۱] و کارکردهای امنیتی را برای شبکه‌های انتقال صدا بر روی پروتکل اینترنتی[۲] (VoIP) فراهم می‌آورد. علاوه بر آن کنترل‌کننده محدوده نشست (SBC) ارتباطات محافظت‌شده‌ای بین مؤلفه‌های امن زیرساخت‌های شبکه فراهم می‌آورد.

مرز[۳] فیزیکی کنترل‌کننده محدوده نشست (SBC) با ذخیره‌سازی مؤلفه‌های سیستم‌عامل یا ارائه توابع امنیتی و تمامی نرم‌افزارهای عرضه‌شده توسط فروشنده (شامل مؤلفه‌های تغییریافته فروشنده برای سیستم‌عامل) تعریف‌شده است. تمامی قابلیت‌های کارکردی امنیتی در درون مرزهای فیزیکی افزاره گنجانده و اجرا می‌شوند.

در اینجا شرح مختصری از قابلیت‌های کارکردی آورده شده است که محصول عهده‌دار پیاده‌سازی آن‌ها جهت پاسخ به تهدیدات محیطی موردبحث در بخش‌های بعدی است. یک محصول منطبق با پروفایل حفاظتی، قابلیت‌های کارکردی امنیتی را ارائه خواهد داد که تهدیدات متوجه خود را موردبررسی قرار می‌دهد. همچنین محصول باید با استفاده از کانال امن از ارتباطات بین خود و تبادل انشعاب خصوصی با پروتکل اینترنتی[۴] (IP PBX) یا کنترل‌کننده محدوده نشست (SBC) دیگری

---

[۱] interoperability

[۲] Voice over Internet Protocol

[۳] boundary

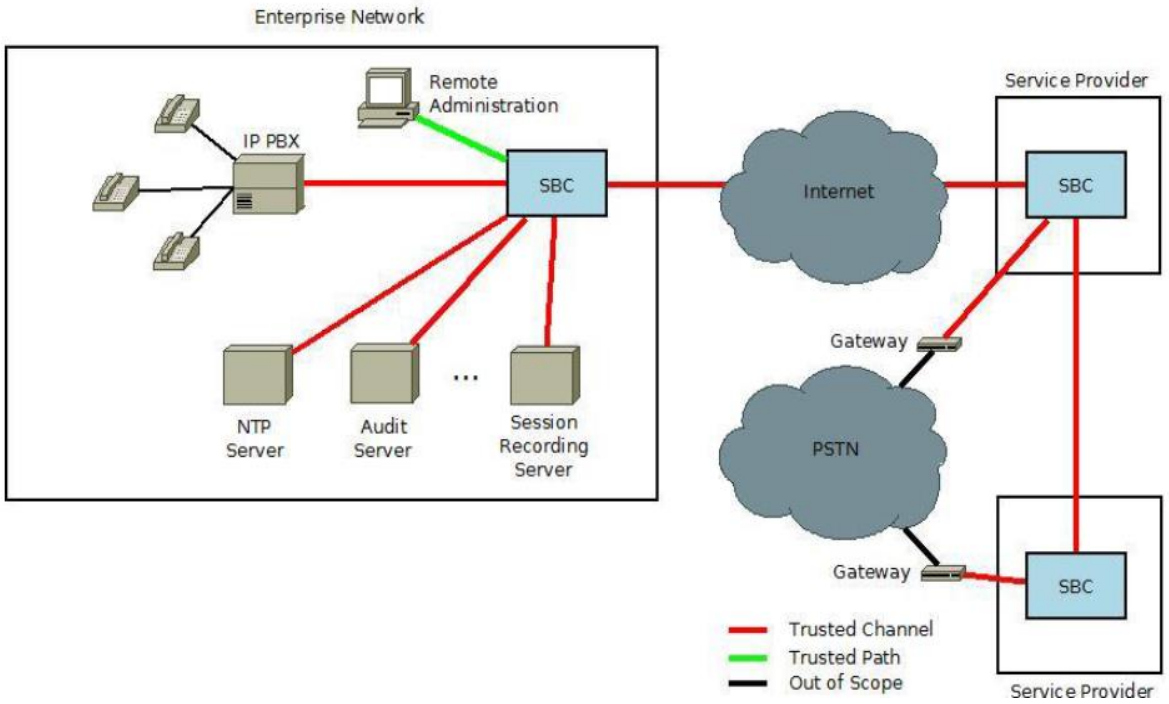
[۴] Private Branch Exchange with Internet Protocol

محافظت کند. برخی از پروتکل‌های موردنیاز این بسته الحاقی از گواهی‌هایی استفاده می‌کنند، بنابراین کنترل‌کننده محدوده نشست (SBC) باید به‌صورت امن گواهی‌ها و کلیدهای خصوصی را ذخیره کند.

از آنجا که این بسته الحاقی بر اساس پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) نوشته‌شده است، محصول منطبق، متعهد به پیاده‌سازی قابلیت‌های کارکردی موردنیاز در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) به همراه قابلیت‌های کارکردی اضافی تعریف‌شده در این بسته الحاقی در پاسخ به تهدیدات محیطی موردبحث در بخش‌های بعدی این سند است.

۲-۲- سناریوی گسترش

کنترل‌کننده محدوده نشست (SBC)، یک افزاره امنیتی است که از سخت‌افزار و نرم‌افزار متصل به دو یا چند شبکه مجزای صدا تشکیل‌شده که کارکردهای امنیتی و قابلیت تبادل و استفاده از اطلاعات را فراهم می‌آورد. کنترل‌کننده‌های محدوده نشست (SBC)، بین شبکه‌های ارائه‌دهنده خدمات مشابه، شبکه‌های ارائه‌دهنده خدمات و شبکه‌های سازمانی، یا شبکه‌های ارائه‌دهنده خدمات و مشتریان محلی گسترش می‌یابند.



شکل ۱ مدل گسترش کنترل‌کننده محدوده نشست (SBC)

۳- تعریف مسئله امنیتی

کنترل‌کننده محدوده نشست (SBC) یک افزاره شبکه‌ای تخصصی است که خدمات دیواره آتش را برای انتقال صدا بر روی شبکه‌های پروتکل اینترنتی (VoIP) فراهم می‌آورد. کنترل‌کننده محدوده نشست (SBC)، برای محافظت در مقابل تهدیدات خوب شناخته‌شده در نظر گرفته‌شده که این شبکه‌ها را هدف قرار داده‌اند.

کنترل‌کننده محدوده نشست (SBC) سربرگ‌ها[۱] و مقادیر داده بسته‌ها را موردبررسی قرار داده و آن‌ها را با یک فهرست کنترل دسترسی[۲] (ACL) مقایسه می‌کند تا اجازه ورود آن‌ها را به کنترل‌کننده محدوده نشست (SBC) و یا عبور از کنترل‌کننده محدوده نشست (SBC) صادر کند یا رد کند. کنترل‌کننده محدوده نشست (SBC) معمولاً در ارتباط بین ارائه‌دهندگان خدمات؛ برای اهداف امنیتی، تبادل و استفاده از اطلاعات، برگردان و تبدیل کد گسترش می‌یابد؛ در ارتباط بین ارائه‌دهندگان خدمات و مشتریان محلی؛ برای اهداف امنیتی، تبادل و استفاده از اطلاعات گسترش‌یافته؛ و یا در ارتباط بین ارائه‌دهندگان خدمات و شبکه‌های سازمانی برای اهداف ترجمه، تبدیل کد و اهداف امنیتی گسترش می‌یابد. کنترل‌کننده محدوده نشست (SBC) به‌عنوان یک عنصر مرزی، باید قادر به برقراری یک کانال ارتباطی امن برای ارتباط با افزاره‌های خارجی باشد.

این بسته الحاقی، الزامات کارکردی و تهدیدات خاص را برای یک کنترل‌کننده محدوده نشست (SBC) تشریح می‌کند. الزامات کارکردی اضافی مرتبط به کنترل‌کننده محدوده نشست (SBC) که به‌عنوان یک افزاره شبکه در حال کار است، در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مشخص‌شده است که در اینجا تکرار نمی‌شود. تمامی الزامات کارکردی در کنترل‌کننده محدوده نشست (SBC) اعمال می‌شود حتی اگر در این بسته الحاقی مشخص نشده باشد، مگر اینکه به‌صراحت حذف‌شده باشد.

۳-۱- تهدیدات

به‌عنوان یک الحاقیه بر پروفایل حفاظتی مشترک افزاره شبکه، کنترل‌کننده محدوده نشست (SBC) با همان تهدیداتی روبرو خواهد بود که به‌طورکلی برای همه افزاره‌های شبکه به کار می‌رود. با این حال با توجه به ماهیت خاص ترافیک به کار گرفته‌شده توسط کنترل‌کننده محدوده نشست (SBC)، برخی از این تهدیدات در محتوای خاص‌تری کاربردپذیر هستند.

---

[۱] Header

[۲] Access Control List

تهدیدات	توضیحات
تهدید افشای شبکه T.NETWORK_DISCLOSURE	افزاره‌های موجود در شبکه حفاظت‌شده ممکن است در معرض تهدیداتی قرار گیرند که توسط افزاره‌هایی ارائه‌شده باشد که در خارج از شبکه محافظت‌شده، قرار دارند و در تلاش برای انجام فعالیت‌های غیرمجاز هستند. اگر افزاره‌های خارجی مخرب شناخته‌شده‌ای قادر به برقراری ارتباط با افزاره موجود در شبکه محافظت‌شده باشند، یا اگر افزاره‌های موجود در شبکه محافظت‌شده، بتوانند ارتباطاتی با آن افزاره‌های خارجی برقرار کنند، ممکن است افزاره‌های داخلی در معرض خطر افشای غیرمجاز اطلاعات شناسایی کننده خود و یا خدمات در دسترس شبکه قرار گیرند. کنترل‌کننده محدوده نشست (SBC)، به‌عنوان یک عامل کاربر پشت‌به‌پشت[۱] (B2BUA) به کار می‌رود که مانع از ارتباط مستقیم موجودیت‌های خارجی با موجودیت‌های داخلی (محافظت‌شده) می‌شود. کنترل‌کننده محدوده نشست (SBC) به‌عنوان یک پیشکار[۲] عمل می‌کند که در آن تنها راه ارتباطی که یک موجودیت خارجی می‌تواند با یک موجودیت محافظت‌شده ارتباط برقرار کند درخواست از کنترل‌کننده محدوده نشست (SBC) برای ارتباط با موجودیت محافظت‌شده از طرف آن موجودیت است. کنترل‌کننده محدوده نشست (SBC) به‌منظور تسهیل ارتباطات، دو اتصال جداگانه را برقرار می‌کند: یکی اتصال با موجودیت خارجی و یکی اتصال با موجودیت حفاظت‌شده داخلی. علاوه بر این، دسترسی می‌تواند

[۱] Back-to-back user agent

[۲] proxy

	محدود به نشانی‌های منابع خاص و پورت‌ها باشد به‌گونه‌ای که دسترسی شبکه‌های خاص یا گره‌های شبکه به شبکه حفاظت‌شده قابل مسدود کردن باشد و بدین ترتیب افشای غیرمجاز اطلاعات بالقوه را محدود کرد. عامل تهدید افشای شبکه (T.NETWORK_DISCLOSURE) مهاجمی است که ممکن است در تلاش برای ترسیم یک زیر شبکه باشد تا افزاره‌هایی را که در شبکه مستقر هستند تعیین کند و نشانی پروتکل اینترنتی ماشین‌ها و همچنین خدماتی (پورت‌هایی) را که آن ماشین‌ها ارائه می‌دهند به دست آورد. این اطلاعات ممکن است برای شروع حملات به آن ماشین‌ها از طریق خدمات در معرض خطر استفاده شود.
ترافیک مخرب T.MALICIOUS_TRAFFIC	کنترل‌کننده محدوده نشست (SBC)، محافظت در برابر بسته‌های مخرب و یا ناقص را فراهم می‌کند. بسته‌های ناقص می‌تواند موجب شوند محصول، یا افزاره‌هایی که محصول از آن‌ها محافظت می‌کند، اجازه دسترسی‌های غیرمجاز را داده و یا باعث انکار خدمت[۱] (DoS) شوند. تهدید ترافیک مخرب (T.MALICIOUS_TRAFFIC) یک مهاجم است که ممکن است اقدام به ارسال بسته‌های ناقص به کنترل‌کننده محدوده نشست (SBC) کند تا باعث شنود پشته شبکه یا خدمات از پورت‌های UDP/TCP بر روی کنترل‌کننده محدوده نشست (SBC) و یا درهم شکستن شبکه حفاظت‌شده شود.
کانال‌های ارتباطی غیر امن T.UNTRUSTED_COMMUNICATION_CHANNELS	یک افزاره عمومی شبکه ممکن است با استفاده از کانال‌های ارتباطی ناامن برای انتقال داده حساس مورد تهدید قرار گیرد. سطح ظاهری[۲] حمله به کنترل‌کننده محدوده نشست (SBC)، ممکن است شامل ارتباطات امنی

[۱] Denial of Service

[۲] Surface

	باشد که خاص داده کاربری انتقال‌یافته از طریق محصول است. عدم توانایی در امن نگه‌داشتن کانال‌های ارتباطی، یا شکست در انجام درست آن، داده کاربری که فرض می‌شود امن باشد را در معرض افشای غیرمجاز قرار خواهد داد. تهدید کانال ارتباطی غیر امن (T.UNTRUSTED_COMMUNICATION_CHANNELS)، مهاجمی است که ممکن است به دلیل وجود کانال ارتباطی غیر امنی که باعث افشای داده در حین انتقال شده است به داده حساس محصول و یا کاربر که به/از محصول انتقال‌یافته، دست یابد.
دسترسی به شبکه T.NETWORK_ACCESS	کنترل‌کننده محدوده نشست (SBC)، به‌عنوان افزاره‌ای که در حاشیه شبکه می‌نشیند، دارای یک رابط رو به خارج به شبکه عمومی است. افزاره‌های واقع در شبکه عمومی ممکن است اقدام به اجرای خدمات قرارگرفته در شبکه داخلی کند که این خدمات برای دسترسی تنها در درون شبکه داخلی در نظر گرفته‌شده‌اند و یا تنها از طریق افزاره‌های مجاز خاصی قابل‌دسترسی هستند. اگر کنترل‌کننده محدوده نشست (SBC) اجازه دسترسی افزاره‌های خارجی غیرمجاز را به شبکه داخلی بدهد، افزاره‌های داخلی ممکن است در معرض خطر قرار بگیرند. تهدید دسترسی به شبکه (T.NETWORK_ACCESS) مهاجمی است که ممکن است ترافیک را از طریق محصولی ارسال کند که آن‌ها را قادر به دسترسی بدون مجوز به افزاره‌های موجود در محیط عملیاتی محصول می‌کند.

استفاده مجدد از داده کاربر T.USER_DATA_REUSE	به‌عنوان قسمتی از عامل B2BUA، کنترل‌کننده محدوده نشست (SBC) مسئول حصول اطمینان از این موضوع است که ارتباطات از موجودیت‌های از راه دور تنها به گیرنده (های) مجاز معطوف است. شکست در انجام این کار باعث افشای غیرعمدی داده کاربر در حال گذر از محصول می‌شود. در تهدید استفاده مجدد از داده کاربر (T.USER_DATA_REUSE)، ممکن است داده کاربر به‌صورت غیر عمد به مقصدی که مدنظر فرستنده اصلی نیست فرستاده شود که باعث افشای غیرمجاز داده می‌شود.
تحلیل رفتن[۱] منابع T.RESOURCE_EXHAUSTION	کنترل‌کننده محدوده نشست (SBC)، مسئول تسهیل ارتباطات بین افزاره‌ها در محیط عملیاتی است. هرچند، کنترل‌کننده محدوده نشست (SBC) دارای منابع محدودی جهت انجام این کار است. چنانچه این منابع به‌وسیله عوامل مخرب دچار فرسودگی شوند، کنترل‌کننده محدوده نشست (SBC) قادر به تسهیل ارتباطات VoIP نخواهد بود. عامل تهدید (T.RESOURCE_EXHAUSTION)، مهاجمی است که ممکن است ترافیک شبکه را به محصول انتقال دهد و باعث شود که محصول قادر به اجرای کارکردهای خود بر روی ترافیک شبکه مشروع نباشد.

۳-۲- مفروضات

مفروضات تعریف‌شده برای محیط عملیاتی کنترل‌کننده محدوده نشست (SBC) با مفروضات تعریف‌شده برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) به‌استثنای مورد زیر یکسان است:

[۱] Exhaustion

فرض امنیتی	توضیحات
عدم حفاظت سرتاسری ترافیک A.NO_THRU_TRAFFIC_PROTECTION	فرض عدم حفاظت سرتاسری ترافیک (A.NO_THRU_TRAFFIC_PROTECTION) که در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تعریف‌شده است، برای این بسته الحاقی کاربردی ندارد. کنترل‌کننده محدوده نشست (SBC) برای ارائه بازرسی عمیق بسته (DPI)[۱] بر روی ترافیک عبور کننده از رابط‌هایش در نظر گرفته‌شده است. بازرسی عمیق بسته (DPI) از گیرنده مقصد و خود در برابر ترافیک مخرب محافظت می‌کند. همچنین کنترل‌کننده محدوده نشست (SBC) به‌عنوان نقطه پایانی رمزگذاری به کار می‌رود. کنترل‌کننده محدوده نشست (SBC) باید به‌درستی رمزگشایی کرده و از ترافیک ورودی رابط‌هایش و رمزگذاری مجدد و از ترافیک خروجی رابط‌های خودش محافظت کند.

۴- اهداف امنیتی

۴-۱- اهداف امنیتی محصول

تهدیدات توصیف‌شده در بخش ۳، با ترکیبی از قابلیت‌های کارکردی محصول و مشخصه‌های محیط عملیاتی محصول، تضعیف خواهند شد. هدف‌های ارزیابی منطبق، قابلیت‌های کارکرد امنیتی‌ای ارائه خواهند داد که تهدیدات محصول را موردتوجه قرار داده و هر خط‌مشی اعمال‌شده توسط قوانین و مقررات را به کار می‌بندد. در ادامه اهداف امنیتی موردنیاز جهت رویارویی با تهدیدات و خط‌مشی‌هایی که قبلاً موردبحث قرارگرفته تشریح خواهند شد.

نکته: اهداف امنیتی خاص (که با .O نشان داده‌شده‌اند) در زیر بخش‌های پیش‌رو مشخص‌شده‌اند. این اهداف با الزامات کارکرد امنیتی (SFR) مرتبط که سازوکارهایی برای برآوردن اهداف، فراهم می‌آورند منطبق هستند. این الزامات شامل الزامات کارکرد امنیتی است که به‌طور خاص برای این بسته الحاقی

[۱] Deep Packet Inspection

تعریف‌شده‌اند (بخش ۵-۲-۲ را ببینید) و همچنین شامل الزامات کارکرد امنیتی پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا است که یا در این بسته الحاقی پالایش‌شده‌اند و یا در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا اختیاری بوده ولی برای این بسته الحاقی اجباری است (بخش ۵-۲-۱ را ببینید).

هدف امنیتی	توضیحات
سامانه ناظر O.SYSTEM_MONITORING	به‌منظور اطمینان از شناسایی فعالیت مخرب بالقوه، پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) نیاز دارد تا رویدادهای مرتبط با امنیت مورد ممیزی قرار گیرند. همچنین کنترل‌کننده محدوده نشست (SBC) توابع امنیتی را برای پشتیبانی از سامانه ناظر فراهم کرده، رویدادهای مرتبط با امنیتی بیشتری را برای توابع خاص کنترل‌کننده محدوده نشست (SBC) تعریف می‌کند و خواستار استفاده از یک سرور پروتکل زمانی شبکه (NTP) جهت ارائه زمان دقیق سامانه است. همچنین انتظار می‌رود کنترل‌کننده محدوده نشست (SBC) با ارائه توانایی تولید خودکار هشدار در زمان وقوع انواع معینی از رویدادها از سامانه ناظر بلادرنگ پشتیبانی کند. هدف امنیتی سامانه ناظر (O.SYSTEM_MONITORING) با الزامات کارکرد امنیتی هشدارهای امنیتی (FAU_ARP.1)، تولید داده ممیزی (FAU_GEN.1)، تحلیل تخلف بالقوه (FAU_SAA.1) و مهرهای زمانی مطمئن (FPT_STM.1) در ارتباط است: (O.SYSTEM_MONITORING :FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FPT_STM.1)
ارتباطات حفاظت‌شده O.PROTECTED_COMMUNICATIONS	برای تضعیف تهدید افشای داده در حال انتقال، کنترل‌کننده محدوده نشست (SBC) باید اطمینان حاصل کند که ارتباطات از راه دور با استفاده از ابراز مناسبی امن شده‌اند. این ابزارها شامل امنیت سیگنال دهی VoIP، کانال‌های رسانه‌ای و برقراری ارتباط با کانال دهی پروتکل آغاز نشست (SIP)، به‌اضافه هر کانال ارتباطاتی امنی است که توسط پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا تعیین‌شده است (مانند ارتباطات با سرورهای ممیزی، سرورهای احراز هویت و یا سرورهای به‌روزرسانی و همچنین رابط‌های اجرایی از راه دور).

	هدف امنیتی ارتباطات حفاظت‌شده (O.PROTECTED_COMMUNICATIONS) با الزامات کارکرد امنیتی عملیات رمزنگاری (رمزگذاری / رمزگشایی داده استاندارد رمزگذاری پیشرفته) (FCS_COP.1(1))، امنیت لایه انتقال دیتاگرام (FCS_DTLS_EXT.1)، امنیت پروتکل اینترنتی (FCS_IPSEC_EXT.1)، پروتکل انتقال بلادرنگ امن (FCS_SRTP_EXT.1)، کانال دهی پروتکل شروع نشست (FIA_SIPT_EXT.1)، پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت (FCS_TLSC_EXT.2)، پروتکل سرویس‌دهنده امنیت لایه انتقال با احراز هویت (FCS_TLSS_EXT.2)، کانال امن درون محصول (FTP_ITC.1) و عناصر ۲، ۳ و ۴ این الزام در ارتباط است: (O.PROTECTED_COMMUNICATIONS: FCS_COP.1(1), FCS_DTLS_EXT.1, FCS_IPSEC_EXT.1, FCS_SRTP_EXT.1, FIA_SIPT_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.2, FTP_ITC.1, FTP_ITC.1(2), FTP_ITC.1(3), FTP_ITC.1(4)
پنهان کردن همبندی[۱] O.TOPOLOGY_HIDING	به‌منظور حصول اطمینان از این‌که هیچ افشای غیرمجازی از اطلاعات شبکه وجود ندارد، انتظار می‌رود کنترل‌کننده محدوده نشست (SBC) همبندی شبکه محافظت‌شده را پنهان کند. کنترل‌کننده محدوده نشست (SBC)، اطمینان حاصل می‌کند که با کار کردن به‌عنوان عامل کاربر پشت‌به‌پشت (B2BUA) و با ارائه پشتیبانی از برگردان نشانی شبکه (NAT) هیچ افشای غیرمجازی وجود ندارد. این سازوکارها اطمینان حاصل می‌کنند که دریافت‌کننده موردنظر برای داده انتقال‌یافته از طریق محصول آشکار نشده و افزاره‌های موجود در شبکه حفاظت‌شده مستقیماً قابل‌دسترسی نیستند. هدف امنیتی پنهان کردن همبندی (O.TOPOLOGY_HIDING) با الزامات کارکرد امنیتی خط‌مشی کنترل جریان اطلاعات (FDP_IFC.1)، توابع کنترل جریان اطلاعات (FDP_IFF.1) و پنهان کردن همبندی (ریخت‌شناسی) یا پیمایش برگردان نشانی شبکه (FFW_NAT_EXT.1) در ارتباط است: (O.TOPOLOGY_HIDING: FDP_IFC.1, FDP_IFF.1, FFW_NAT_EXT.1)

[۱] Topology

O.TRAFFIC_FILTERING پالایش[۱] ترافیک	برای حصول اطمینان از اینکه ترافیک مخرب نمی‌تواند کنترل‌کننده محدوده نشست (SBC) و یا افزاره‌های موجود در درون شبکه محافظت‌شده را در معرض خطر قرار دهند، انتظار می‌رود کنترل‌کننده محدوده نشست (SBC)، قابلیت‌های پالایش ترافیک اولیه را ارائه دهد. این کار اطمینان حاصل می‌کند که ترافیک غیرمجاز TCP/UDP مسدود شده و تمام ترافیک سیگنال دهی و رسانه‌ای در ابتدا و قبل از انجام هرگونه اقدامی بر روی آن، موردبررسی قرار می‌گیرد تا به‌خوبی شکل‌گرفته باشد. هدف امنیتی پالایش ترافیک (O.TRAFFIC_FILTERING) با الزامات کارکرد امنیتی پالایش ترافیک VoIP (FFW_ACL_EXT.1)، پالایش ترافیک VoIP وضعیت (حالت دار) (FFW_ACL_EXT.2) و بازرسی عمیق بسته (FFW_DPI_EXT.1) در ارتباط است: (O.TRAFFIC_FILTERING: FFW_ACL_EXT.1, FFW_ACL_EXT.2, FFW_DPI_EXT.1)
تحویل داده کاربر O.USER_DATA_DELIVERY	هنگامی که داده کاربر بین طرف‌های تماس‌گیرنده انتقال می‌یابد، طرف‌های تماس‌گیرنده انتظار دارند که این داده تنها به دریافت‌کننده (گان) موردنظر انتقال یابد. انتظار می‌رود کنترل‌کننده محدوده نشست (SBC) این تضمین را از طریق عملکرد صحیح به‌عنوان یک عامل B2BUA و پیاده‌سازی صحیح پروتکل آغاز نشست (SIP) فراهم آورد. هدف امنیتی تحویل داده کاربر (O.USER_DATA_DELIVERY) با الزامات کارکرد امنیتی خط‌مشی کنترل جریان اطلاعات (FDP_IFC.1)، توابع کنترل جریان اطلاعات (FDP_IFF.1)، پنهان کردن همبندی (ریخت‌شناسی) یا پیمایش برگردان نشانی شبکه ((FFW_NAT_EXT.1، سرور پروتکل آغاز نشست (FIA_SIPS_EXT.1) و کانال دهی پروتکل شروع نشست (FIA_SIPT_EXT.1) در ارتباط است: (O.USER_DATA_DELIVERY: FDP_IFC.1, FDP_IFF.1, FFW_NAT_EXT.1, FIA_SIPS_EXT.1, FIA_SIPT_EXT.1)

[۱] filtering

دسترس‌پذیری منابع O.RESOURCE_AVAILABILITY	اگر مهاجمی بتواند با یک حمله انکار خدمت (DoS) مانع ساماندهی داده کاربر توسط کنترل‌کننده محدوده نشست (SBC) شود، کنترل‌کننده محدوده نشست (SBC) قادر به اجرای قابلیت‌های کارکردی اصلی خود نخواهد بود؛ بنابراین انتظار می‌رود کنترل‌کننده محدوده نشست (SBC) توابع امنیتی‌ای را ارائه دهد که اجازه اولویت‌بندی منابعش و محافظت در مقابل ترافیکی که تنها برای ایجاد اختلال در دسترس‌پذیری افزاره طراحی‌شده است را بدهد. هدف امنیتی دسترس‌پذیری منابع (O.RESOURCE_AVAILABILITY) با الزامات کارکرد امنیتی اولویت محدودشده سرویس (FRU_PRS_EXT.1) و حداکثر سهمیه‌ها (FRU_RSA.1) در ارتباط است: (O.RESOURCE_AVAILABILITY: FRU_PRS_EXT.1, FRU_RSA.1)
مدیریت مجاز O.AUTHORIZED_ADMINISTRATION	انتظار می‌رود تمامی افزاره‌های شبکه خدماتی را ارائه دهند که به قابلیت‌های کارکردی امنیتی افزاره اجازه دهد که مدیریت شوند. کنترل‌کننده محدوده نشست (SBC)، به‌عنوان یک نوع خاص افزاره شبکه، مجموعه‌ای از توابع مدیریتی پالایش‌شده را در برمی‌گیرد که رفتار خاص آن را موردتوجه قرار می‌دهد. هدف امنیتی مدیریت مجاز (O.AUTHORIZED_ADMINISTRATION) با الزام کارکرد امنیتی مشخصات توابع مدیریت (FMT_SMF.1) در ارتباط است: (O.AUTHORIZED_ADMINISTRATION: FMT_SMF.1)

۴-۲- اهداف امنیتی محیط عملیاتی

اهداف امنیتی محیط عملیاتی برای این بسته الحاقی، همان اهداف امنیتی محیط عملیاتی پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا هستند به‌استثنای هدف امنیتی محیط عملیاتی عدم حفاظت سرتاسر ترافیک (OE.NO_THRU_TRAFFIC_PROTECTION) که از این بسته الحاقی حذف‌شده است. چرا که کنترل‌کننده محدوده نشست (SBC) حفاظت سرتاسر ترافیک را ارائه می‌دهد.

۵- الزامات کارکرد امنیتی

الزامات کارکرد امنیتی (SFR) موجود در این بخش از بخش ۲ معیار مشترک برای ارزیابی امنیت فناوری اطلاعات، نسخه ۳,۱، بازنگری ۴، به همراه مؤلفه‌های کارکردی افزوده، گرفته‌شده است. این الزامات در جدول ۱ قابل‌مشاهده هستند. با توجه به اینکه الزامات کارکردی در این بسته الحاقی یا الزامات موجود در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا هستند که با تغییری با توجه به محصول در اینجا ذکرشده‌اند، یا الزاماتی هستند که خاص محصول هستند، لذا ستون چهارم جدول ۱ برای نشان دادن این دسته‌بندی به جدول افزوده‌شده است. NDcPP نشان‌دهنده الزامات پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا و TOE نشان‌دهنده الزامات خاص محصول است.

جدول ۱ الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد	
۱	تولید داده ممیزی ۱	FAU_GEN.1	NDcPP
۲	عملیات رمزنگاری(رمزگذاری/ رمزگشایی داده استاندارد رمزگذاری پیشرفته) ۱	FCS_COP.1(1)	NDcPP
۳	امنیت پروتکل اینترنتی ۱	FCS_IPSEC_EXT.1	NDcPP
۴	پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت ۱	FCS_TLSC_EXT.2	NDcPP
۵	پروتکل سرویس‌دهنده امنیت لایه انتقال با احراز هویت ۱	FCS_TLSS_EXT.2	NDcPP
۶	مشخصات کارکرد مدیریتی ۱	FMT_SMF.1	NDcPP
۷	پالایش مهرهای زمانی امن ۱	FPT_STM.1.1	NDcPP
۸	کانال امن درون محصول ۱	FTP_ITC.1.1	NDcPP
۹	هشدارهای امنیتی ۱	FAU_ARP.1.1	TOE
۱۰	تحلیل تخلف بالقوه ۱	FAU_SAA.1.1	TOE
۱۱	تحلیل تخلف بالقوه ۲	FAU_SAA.1.2	TOE
۱۲	امنیت لایه انتقال دیتاگرام ۱	FCS_DTLS_EXT.1.1	TOE
۱۳	امنیت لایه انتقال دیتاگرام ۲	FCS_DTLS_EXT.1.2	TOE
۱۴	پروتکل انتقال بلادرنگ امن ۱	FCS_SRTP_EXT.1.1	TOE
۱۵	پروتکل انتقال بلادرنگ امن ۲	FCS_SRTP_EXT.1.2	TOE
۱۶	پروتکل انتقال بلادرنگ امن ۳	FCS_SRTP_EXT.1.3	TOE
۱۷	پروتکل انتقال بلادرنگ امن ۴	FCS_SRTP_EXT.1.4	TOE
۱۸	خط‌مشی کنترل جریان اطلاعات ۱	FDP_IFC.1.1	TOE
۱۹	توابع کنترل جریان اطلاعات ۱	FDP_IFF.1.1	TOE

شماره الزام	نام الزام	تطابق الزام با استاندارد	
۲۰	توابع کنترل جریان اطلاعات ۲	FDP_IFF.1.2	TOE
۲۱	توابع کنترل جریان اطلاعات ۳	FDP_IFF.1.3	TOE
۲۲	توابع کنترل جریان اطلاعات ۴	FDP_IFF.1.4	TOE
۲۳	توابع کنترل جریان اطلاعات ۵	FDP_IFF.1.5	TOE
۲۴	پالایش ترافیک VoIP ۱	FFW_ACL_EXT.1.1	TOE
۲۵	پالایش ترافیک VoIP ۲	FFW_ACL_EXT.1.2	TOE
۲۶	پالایش ترافیک VoIP ۳	FFW_ACL_EXT.1.3	TOE
۲۷	پالایش ترافیک VoIP ۴	FFW_ACL_EXT.1.4	TOE
۲۸	پالایش ترافیک VoIP ۵	FFW_ACL_EXT.1.5	TOE
۲۹	پالایش ترافیک VoIP ۶	FFW_ACL_EXT.1.6	TOE
۳۰	پالایش ترافیک VoIP ۷	FFW_ACL_EXT.1.7	TOE
۳۱	پالایش ترافیک VoIP وضعیت (حالت‌دار) ۱	FFW_ACL_EXT.2.1	TOE
۳۲	پالایش ترافیک VoIP وضعیت (حالت‌دار) ۲	FFW_ACL_EXT.2.2	TOE
۳۳	پالایش ترافیک VoIP وضعیت (حالت‌دار) ۳	FFW_ACL_EXT.2.3	TOE
۳۴	پالایش ترافیک VoIP وضعیت (حالت‌دار) ۴	FFW_ACL_EXT.2.4	TOE
۳۵	پالایش ترافیک VoIP وضعیت (حالت‌دار) ۵	FFW_ACL_EXT.2.5	TOE
۳۶	بازرسی عمیق بسته ۱	FFW_DPI_EXT.1.1	TOE
۳۷	بازرسی عمیق بسته ۲	FFW_DPI_EXT.1.2	TOE
۳۸	بازرسی عمیق بسته ۳	FFW_DPI_EXT.1.3	TOE
۳۹	پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۱	FFW_NAT_EXT.1.1	TOE

شماره الزام	نام الزام	تطابق الزام با استاندارد	
۴۰	پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۲	FFW_NAT_EXT.1.2	TOE
۴۱	پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۳	FFW_NAT_EXT.1.3	TOE
۴۲	پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۴	FFW_NAT_EXT.1.4	TOE
۴۳	سرور پروتکل آغاز نشست ۱	FIA_SIPS_EXT.1.1	TOE
۴۴	سرور پروتکل آغاز نشست ۲	FIA_SIPS_EXT.1.2	TOE
۴۵	سرور پروتکل آغاز نشست ۳	FIA_SIPS_EXT.1.3	TOE
۴۶	سرور پروتکل آغاز نشست ۴	FIA_SIPS_EXT.1.4	TOE
۴۷	کانال دهی پروتکل شروع نشست ۱	FIA_SIPT_EXT.1.1	TOE
۴۸	کانال دهی پروتکل شروع نشست ۲	FIA_SIPT_EXT.1.2	TOE
۴۹	کانال دهی پروتکل شروع نشست ۳	FIA_SIPT_EXT.1.3	TOE
۵۰	کانال دهی پروتکل شروع نشست ۴	FIA_SIPT_EXT.1.4	TOE
۵۱	اولویت‌بندی محدود خدمت ۱	FRU_PRS_EXT.1.1	TOE
۵۲	اولویت‌بندی محدود خدمت ۲	FRU_PRS_EXT.1.2	TOE
۵۳	حداکثر سهمیه ۱	FRU_RSA.1.1	TOE
۵۴	کانال امن درون محصول(۲) ۱	FTP_ITC.1(2).1	TOE
۵۵	کانال امن درون محصول(۲) ۲	FTP_ITC.1(2).2	TOE
۵۶	کانال امن درون محصول(۲) ۳	FTP_ITC.1(2).3	TOE
۵۷	کانال امن درون محصول(۳) ۱	FTP_ITC.1(3).1	TOE
۵۸	کانال امن درون محصول(۳) ۲	FTP_ITC.1(3).2	TOE
۵۹	کانال امن درون محصول(۳) ۳	FTP_ITC.1(3).3	TOE

شماره الزام	نام الزام	تطابق الزام با استاندارد	
۶۰	**کانال امن درون محصول(۴) ۱**	FTP_ITC.1(4).1	TOE
۶۱	**کانال امن درون محصول(۴) ۲**	FTP_ITC.1(4).2	TOE
۶۲	**کانال امن درون محصول(۴) ۳**	FTP_ITC.1(4).3	TOE

۵-۱- قراردادها

معیار مشترک عملیات بر روی الزامات کارکرد امنیتی را این‌گونه تعریف می‌کند: اختصاص، انتخاب، اختصاص درون انتخاب و پالایش. این سند از قراردادهای فونتی زیر برای شناسایی عملیات تعریف‌شده توسط معیار مشترک استفاده می‌کند:

- اختصاص: با *متن مایل* نشان داده می‌شود.
- پالایش ایجادشده توسط نویسنده بسته الحاقی: با **متن پررنگ** نشان داده می‌شود.
- انتخاب: با متن زیرخط دار نشان داده می‌شود.
- اختصاص درون یک انتخاب: با *متن مایل و زیرخط دار* نشان داده می‌شود.
- تکرار: با افزودن تعداد تکرار در پرانتز نشان داده می‌شود مثلاً (۳).
- الزامات کارکرد امنیتی توسعه‌یافته با داشتن برچسب "EXT" بعد از نام الزام در الزامات کارکرد امنیتی محصول شناخته می‌شوند.

۵-۲- الزامات کارکرد امنیتی محصول

به دلیل اینکه این بسته الحاقی از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) توسعه‌یافته است، انتظار می‌رود که این بسته الحاقی توابع امنیتی تعریف‌شده در پروفایل حفاظتی مبنا را به ارث برد. برای آن دسته از توابعی که در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تعریف‌شده‌اند ولی با جزئیات بیشتری در بسته الحاقی مشخص‌شده‌اند، الزامات کارکرد امنیتی به‌روز شده در بخش ۵-۲-۱ زیر ذکرشده است.

۵-۲-۱- جهت‌گیری الزامات کارکردی امنیتی پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)

این بخش دستورالعمل‌هایی را برای نویسنده هدف امنیتی ارائه می‌دهد تا نشان دهد چه انتخاب‌هایی باید برای الزامات کارکرد امنیتی معین گنجانده‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) صورت گیرد تا اهداف امنیتی تعریف‌شده در این بسته الحاقی برآورد شود و یا نشان دهد چگونه تهدیدی را به روش خاص‌تر یا محدودتری نسبت به آنچه در پروفایل حفاظتی مبنا مشخص‌شده است، تضعیف کند.

این دستورالعمل عناصری توصیف می‌کند که در آن انتخابی اجباری شده است. نویسنده هدف امنیتی، ممکن است موارد انتخابی باقیمانده را به‌گونه‌ای انجام دهد تا اطمینان حاصل کند که قابلیت‌ها یا رفتارهای خاصی در محصول موجود است.

تمام اقدامات تضمین برای الزامات این بخش تکرار نمی‌شود بلکه تنها آزمون‌های اضافی موردنیاز برای تکمیل آنچه پیش از این از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) گرفته‌شده است گنجانده‌شده‌اند. هنگامی که ارزیاب هدف امنیتی و محصول را در برابر الزامات کارکرد امنیتی ارزیابی می‌کند، مهم است که انتخاب مناسب انجام گیرد و آزمون‌های مناسبی برای نشان دادن انطباق با الزامات انجام شوند.

۵-۲-۱-۱-کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**
پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)، مجموعه‌ای از رویدادهای قابل ممیزی را تعریف می‌کند که لازم است توسط محصول پیاده‌سازی شود. این بسته الحاقی قابلیت‌های کارکردی اضافی را معرفی می‌کند که گنجاندن رویدادهای قابل ممیزی افزوده‌ای را ضروری می‌کند. رویدادهای جدول ۲ باید با رویدادهای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) ترکیب شوند تا با اهداف امنیتی مطابقت داشته باشند. اگر محصول ادعا کند توانایی تشخیص انحرافات خاصی را به‌عنوان تخلف امنیتی بالقوه در تحلیل تخلف بالقوه (FAU_SAA.1) دارد، نویسنده هدف امنیتی ممکن است به‌طور اختیاری شرایط محیطی مانند تخلف دمایی را تعریف کند. پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)، مستلزم آن است که «تمام اقدامات اداری» ممیزی شوند، نویسنده هدف امنیتی باید این اقدامات اداری را که این بسته الحاقی پشتیبانی می‌کند در متن اختصاص بگنجاند. **نکته کاربردی ۱:** یک رکورد جزئیات تماس[۱] (CDR) باید در آغاز نشست، در پایان نشست و در طول نشست در یک فاصله یا دوره زمانی مشخص‌شده توسط نویسنده هدف امنیتی تولید شود.	

[۱] Call Detail Record

جدول ۲ رویدادهای قابل ممیزی

الزامات کارکرد امنیتی	رویداد قابل ممیزی	مطالب اضافی ضبط حسابرسی
FIA_SIPS_EXT.1	ثبت جزئیات تماس (CDR)	طرف تماس‌گیرنده طرف دریافت‌کننده تماس زمان شروع تماس مدت تماس نوع تماس
FDP_IFF.1	هرگونه تغییرات در خط‌مشی کارکرد امنیتی (SFP) عامل کاربر پشت‌به‌پشت	هیچ
FFW_ACL_EXT.1	پیکربندی قوانین پالایش ترافیک VoIP	اطلاعات منحصربه‌فرد شناسایی کننده قوانینی که اصلاح‌شده‌اند
FIA_SIPS_EXT.1	تمامی درخواست‌های تابع ثبت (REGISTER) پروتکل آغاز نشست (SIP)	هیچ
FIA_SIPT_EXT.1	تمامی تلاش‌های احراز هویت کانال دهی[۱] پروتکل آغاز نشست (SIP)	نام کاربری و نشانی پروتکل اینترنتی ارائه‌دهنده خدمات
FTP_ITC.1(2)	شروع کانال امن، خاتمه دادن کانال امن، شکست توابع کانال امن	شناسایی آغازگر و هدف کانال امن
FTP_ITC.1(3)	شروع کانال امن، خاتمه دادن کانال امن، شکست توابع کانال امن	شناسایی آغازگر و هدف کانال امن
FTP_ITC.1(4)	شروع کانال امن، خاتمه دادن کانال امن، شکست توابع کانال امن	شناسایی آغازگر و هدف کانال امن

۵-۲-۱-۲- کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۲	**عملیات رمزنگاری (رمزگذاری / رمزگشایی داده استاندارد رمزگذاری پیشرفته) ۱**

[۱] trunk

در حال حاضر این الزام کارکرد امنیتی، برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) اجباری است، اما در این بسته الحاقی با توجه به پیاده‌سازی اضافی استاندارد رمزگذاری پیشرفته (AES) توسط یک کنترل‌کننده محدوده نشست (SBC) محصول یادآوری شده است تا به‌عنوان نقطه پایانی رمزگذاری رسانه‌ای به کار گرفته شود که قادر به رمزگشایی و رمزگذاری مجدد داده تماس در حال عبور از میان محصول (TSF) است.	
۳	**امنیت پروتکل اینترنتی ۱**
این الزام کارکرد امنیتی در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) اختیاری است، اما در بسته الحاقی به دلیل استفاده از امنیت پروتکل اینترنتی (IPsec) برای امن کردن سیگنال دهی و کانال رسانه‌ای اجباری شده است.	
۴	**پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت ۱**
این الزام کارکرد امنیتی در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) اختیاری است اما در این بسته الحاقی به دلیل استفاده از امنیت لایه انتقال (TLS) برای کانال دهی پروتکل آغاز نشست (SIP) اجباری شده است.	
۵	**پروتکل سرویس‌دهنده امنیت لایه انتقال با احراز هویت ۱**
این الزام کارکرد امنیتی در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) اختیاری است اما در این بسته الحاقی به دلیل استفاده از امنیت لایه انتقال (TLS) برای کانال دهی پروتکل آغاز نشست (SIP) اجباری شده است.	

۵-۲-۱-۳- کلاس مدیریت امنیت

شماره الزام	نام الزام
۶	**مشخصات کارکرد مدیریتی ۱**

توابع مدیریت افزوده‌شده، الزامات کارکرد امنیتی مشخصات توابع مدیریتی (FMT_SMF.1) موجود در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را توسعه می‌دهد.

توابع زیر باید با توابع موجود در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) در محتوای یک هدف امنیتی منطبق ترکیب شوند.

توانایی‌های یک مدیر سیستم امنیتی شامل موارد زیر است:

- تغییر کلمه عبور کاربر
- درخواست برای تغییر کلمه عبور کاربر به‌محض ورود بعدی
- پیکربندی رویدادهای قابل ممیزی که منجر به تولید یک هشدار خواهند شد.
- پیکربندی خط‌مشی کارکرد امنیتی (SFP) عامل کاربر پشت‌به‌پشت
- پیکربندی قوانین پالایش ترافیک
- پیکربندی برگردان نشانی شبکه (NAT)
- پیکربندی ارتباطات پروتکل آغاز نشست (SIP)
- فعال یا غیرفعال کردن استفاده از الگوریتم SRTP NULL
- مشخص کردن پورت‌های مورداستفاده برای SRTP

۵-۲-۱-۴- کلاس حفاظت از محصول

شماره الزام	نام الزام
۷	**پالایش مهرهای زمانی امن ۱**

محصول (TSF) باید قادر به ارائه مهرهای زمانی مطمئن با استفاده از پروتکل زمانی شبکه[۱] نسخه ۴ (NTPv4) مشخص‌شده در RFC 5905 باشد.

۵-۲-۱-۵- کلاس کانال‌ها/مسیرهای مورد اعتماد

شماره الزام	نام الزام
۸	**کانال امن درون محصول ۱**
محصول باید قادر به استفاده از SNMPv3، SRTP، TLS و [انتخاب: IPsec، SSH، HTTPS، هیچ پروتکل دیگری] برای ارائه یک کانال ارتباطی امن بین خود و دیگر موجودیت‌های فناوری اطلاعات مجاز پشتیبانی‌کننده از قابلیت‌های زیر باشد: سرور ممیزی، سرور NTP، [انتخاب: سرور احراز هویت، اختصاص: [قابلیت‌های دیگر] که منطقاً از دیگر کانال‌های ارتباطی مجزا است و شناسایی مطمئنی از نقاط پایانی و حفاظت از داده کانال در برابر افشا و تشخیص تغییر داده کانال فراهم می‌آورد. **نکته کاربردی ۲:** همان‌طور که در بند ۱۳ از IEEE 802.1AE-2006 اشاره‌شده است برای پیاده‌سازی MACsec به SNMPv3 نیاز است. این الزام کارکرد امنیتی از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) برای گنجاندن در این پروتکل بیشتر اصلاح (پالایش) شده است.	

۵-۲-۲- الزامات کارکرد امنیتی محصول

۵-۲-۲-۱- کلاس ممیزی امنیت

شماره الزام	نام الزام
۹	**هشدارهای امنیتی ۱**

[۱] Network Time Protocol

محصول باید] اقدامات زیر: انتقال گیرنده دریچه به دریچه SNMPv3 در محیط عملیاتی[را به‌محض تشخیص تخلف امنیتی بالقوه انجام دهد.	
۱۰	**تحلیل تخلف بالقوه ۱**
محصول باید قادر به اعمال مجموعه‌ای از قوانین برای نظارت بر رویدادهای ممیزی شده بوده و بر اساس این قوانین، تخلف بالقوه در اجرای الزامات کارکرد امنیتی را نشان دهد.	
۱۱	**تحلیل تخلف بالقوه ۲**
محصول باید قوانین زیر را برای نظارت بر رویدادهای ممیزی شده اعمال کند: أ. جمع‌آوری و یا ترکیب [*اختصاص: زیرمجموعه‌ای از رویدادهای قابل ممیزی تعریف‌شده*]شناخته‌شده برای نشان دادن یک تخلف امنیتی بالقوه؛ ب. [*اختصاص: هر قانون دیگر*] **نکته کاربردی ۳:** نمونه‌هایی از نظارت بر رویدادهای ممیزی شده شامل: شکست احراز هویت، شکست خودآزمایی و یا شکست محیطی است.	

۵-۲-۲-۲- کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۲	**امنیت لایه انتقال دیتاگرام ۱**
محصول باید پروتکل امنیت لایه انتقال دیتاگرام (DTLS) را مطابق با RFC 6347 پیاده‌سازی کند.	
۱۳	**امنیت لایه انتقال دیتاگرام ۲**

محصول باید الزامات پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت (FCS_TLSC_EXT.2) را برای پیاده‌سازی پروتکل امنیت لایه انتقال دیتاگرام (DLTS) اجرا کند، به‌جز در مواردی که با توجه به RFC 6347 به تخلفات اجازه داده‌شده است. **نکته کاربردی ۴:** تفاوت‌های میان پروتکل امنیت لایه انتقال دیتاگرام (DTLS) و پروتکل امنیت لایه انتقال (TLS) در RFC 6347 مشخص‌شده است، به‌جز این موارد این دو پروتکل یکسان هستند. به‌طور خاص برای مشخصه‌های امنیتی کاربردپذیر تعریف‌شده برای محصول، این دو پروتکل متفاوت نیستند؛ بنابراین تمامی نکات کاربردی و اقدامات تضمین ذکرشده برای پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت (FCS_TLSC_EXT.2) برای پیاده‌سازی پروتکل امنیت لایه انتقال دیتاگرام (DTLS) به کار گرفته می‌شود.	
پروتکل انتقال بلادرنگ امن ۱	۱۴
محصول باید پروتکل انتقال بلادرنگ امن[۱] (SRTP) را مطابق با RFC 3711 پیاده‌سازی کند و از توضیحات امنیتی جریان‌های رسانه‌ای[۲] (SDES) مطابق با RFC 4568 استفاده کند تا اطلاعات کلیدی را برای اتصال پروتکل انتقال بلادرنگ امن (SRTP) فراهم آورد.	
پروتکل انتقال بلادرنگ امن ۲	۱۵
محصول باید پروتکل انتقال بلادرنگ امن[۳] (SRTP) را مطابق با RFC 3711 پیاده‌سازی کند و از توضیحات امنیتی جریان‌های رسانه‌ای[۴] (SDES) مطابق با RFC 4568 استفاده کند تا اطلاعات کلیدی را برای اتصال پروتکل انتقال بلادرنگ امن (SRTP) فراهم آورد.	
محصول باید پروتکل انتقال بلادرنگ امن جریان‌های رسانه‌ای (SDES_SRTP) را پیاده‌سازی کند که از دنباله رمزهای AES_CM_128_HMAC_SHA1_80 مطابق با RFC 4568 پشتیبانی می‌کند.	

[۱] Secure Real-time Transport Protocol

[۲] Media Streams

[۳] Secure Real-time Transport Protocol

[۴] Media Streams

نکته کاربردی ۵: این الزام مشخص می‌کند که نشست پروتکل انتقال بلادرنگ امن (SRTP) که برای انتقال ترافیک VoIP مورداستفاده قرار خواهد گرفت طبق یک محاوره جریان‌های رسانه‌ای (SDES) با استفاده از دنباله رمز شناسایی‌شده کلیددار خواهد شد.
۱۶ **پروتکل انتقال بلادرنگ امن ۳**
محصول باید اطمینان حاصل کند که الگوریتم SRTP NULL می‌تواند توسط یک مدیر سیستم امنیتی غیرفعال شود.
۱۷ **پروتکل انتقال بلادرنگ امن ۴**
محصول باید اجازه دهد که پورت‌های پروتکل انتقال بلادرنگ امن (SRTP) که برای ارتباطات پروتکل انتقال بلادرنگ امن (SRTP) استفاده می‌شود توسط یک مدیر سیستم امنیتی مشخص شود

۵-۲-۲-۳- کلاس حفاظت از داده‌های کاربری

شماره الزام	نام الزام
۱۸	**خط‌مشی کنترل جریان اطلاعات ۱**
محصول باید [*خط‌مشی کارکرد امنیتی (SFP) عامل کاربر پشت‌به‌پشت*] را بر روی [زوج‌های تماس‌گیرنده – دریافت‌کننده تماس اقدام کننده جهت برقراری ارتباط از طریق محصول] اجرا کند.	
۱۹	**توابع کنترل جریان اطلاعات ۱**
محصول باید [*خط‌مشی کارکرد امنیتی (SFP) عامل کاربر پشت‌به‌پشت*] را بر اساس انواع موجودیت‌های فعال و مشخصه‌های امنیتی اطلاعات اجرا کند: [*اختصاص: روشی که با آن محصول نقطه پایانی تماس را شناسایی می‌کند*].	
۲۰	**توابع کنترل جریان اطلاعات ۲**

درصورتی‌که قوانین زیر وجود داشته باشد محصول باید اجازه جریان اطلاعات را بین موجودیت‌های فعال کنترل‌شده و اطلاعات کنترل‌شده، از طریق عملیات کنترل‌شده بدهد: [*زمانی که ارتباط معتبری از طریق محصول صورت گیرد، محصول اتصالی بین خود و تماس‌گیرنده برقرار خواهد کرد، محصول اتصال دومی بین خود و دریافت‌کننده تماس برقرار خواهد کرد، محصول تمامی ارتباطاتی را که بین دو نقطه پایانی بیرونی سرتاسر اتصال مناسب دریافت می‌کند را تغییر مسیر خواهد داد*].	
توابع کنترل جریان اطلاعات ۳	۲۱
محصول باید [*قوانین رفتاری قابل تنظیم* • *پیش‌فرض- حالت رد (فهرست سفید): چنانچه تنظیم‌شده باشد، محصول به‌طور ضمنی تمامی جریان‌های اطلاعات را به‌جز برای جریاناتی که به‌صراحت توسط محصول مجاز شده‌اند را انکار می‌کند.* • *پیش‌فرض – حالت پذیرش (فهرست سیاه): اگر تنظیم‌شده باشد، محصول به‌طور ضمنی تمامی جریان‌های اطلاعات را می‌پذیرد به‌جز مواردی که به‌صراحت توسط محصول انکار شده باشند*] را اجرا کند.	
توابع کنترل جریان اطلاعات ۴	۲۲
محصول باید به‌طور صریح بر اساس قوانین زیر اجازه جریان اطلاعات را صادر کند: [*اگر محصول در حالت فهرست سفید در حین عملیات باشد، هر طرف تماسی که در فهرست سفید قرارگرفته باشد، (با شماره تماس، نشانی پروتکل اینترنتی منبع و یا پروتکل‌های ارتباطی قابل‌شناسایی است) به‌صراحت مجاز است*].	
توابع کنترل جریان اطلاعات ۵	۲۳
محصول باید به‌صراحت بر اساس قوانین زیر اجازه جریان اطلاعات را انکار کند: [*اگر محصول در حالت فهرست سیاه در حین عملیات باشد، هر طرف تماسی که در فهرست سیاه قرارگرفته باشد، (با شماره تماس، نشانی پروتکل اینترنتی منبع و یا پروتکل‌های ارتباطی قابل‌شناسایی است) به‌صراحت باید رد شود*].	

۵-۲-۲-۴- کلاس پالایش ترافیک

شماره الزام	نام الزام
۲۴	**پالایش ترافیک VoIP ۱**
محصول باید پالایش ترافیک را بر روی بسته‌های شبکه پردازش‌شده توسط محصول انجام دهد.	
۲۵	**پالایش ترافیک VoIP ۲**
محصول باید اجازه تعریف قوانین پالایش ترافیک را با استفاده از رشته‌های (فیلدهای) پروتکل شبکه زیر بدهد: • ICMPv4 ○ نوع ○ کد • ICMPv6 ○ نوع ○ کد • IPv4 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال • IPv6 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال	

○ [انتخاب: نوع سربرگ بسط یافته IPv6، [اختصاص: فهرستی از رشته‌ها در سربرگ بسط یافته IPv6]، هیچ رشته (فیلد) دیگری] • TCP ○ پورت منبع ○ پورت مقصد • UDP ○ پورت منبع ○ پورت مقصد • رابط مجزا	
پالایش ترافیک VoIP ۳	۲۶
محصول باید اجازه دهد تا عملیات زیر با قوانین پالایش ترافیک در ارتباط باشد: • اجازه یا رها کردن قابلیت ثبت عملیات.	
پالایش ترافیک VoIP ۴	۲۷
محصول باید اجازه دهد قوانین پالایش ترافیک به هر رابط شبکه مجزا اختصاص داده شود.	
پالایش ترافیک VoIP ۵	۲۸
محصول باید: أ. اگر بسته شبکه با یک نشست برقرارشده مجاز برای پروتکل‌های: TCP، UDP،] انتخاب: ICMP، هیچ پروتکل دیگری[مطابقت داشته باشد، بسته شبکه را بدون پردازش اضافی قوانین پالایش ترافیک بر اساس خصیصه‌های بسته شبکه زیر بپذیرد: ۱- TCP: نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد، اعداد دنباله، پرچم‌ها ؛ ۲- UDP: نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد؛	

۳-]انتخاب: "ICMP: نشانی‌های منبع و مقصد، نوع،]انتخاب: کد،]اختصاص: فهرستی از خصیصه‌های منطبق[[، هیچ پروتکل دیگری[ب. حذف جریان‌های ترافیک موجود از مجموعه‌ای از جریان‌های ترافیک برقرارشده بر اساس موارد زیر:]انتخاب: وقفه عدم فعالیت نشست، اتمام جریان اطلاعات مورد انتظار[	
پالایش ترافیک VoIP ۶	۲۹
محصول باید قوانین پالایش ترافیک کاربردپذیر را به ترتیب اجرایی تعریف‌شده پردازش کند.	
پالایش ترافیک VoIP ۷	۳۰
چنانچه قانون مطابقت کننده‌ای شناسایی نشود، محصول باید جریان بسته را رد کند.	
پالایش ترافیک VoIP وضعیت (حالت‌دار) ۱	۳۱
محصول باید پالایش ترافیک وضعیت (حالت‌دار) را بر روی پروتکل‌های VoIP زیر انجام دهد: SIP، H.323(H.225, H.245)، [انتخاب: [اختصاص: پروتکل‌های دیگر]، هیچ پروتکل دیگری].	
پالایش ترافیک VoIP وضعیت (حالت‌دار) ۲	۳۲
محصول باید قوانین پالایش ترافیک وضعیت (حالت‌دار) پیش‌فرض زیر را بر روی تمام ترافیک شبکه منطبق بر انواع پروتکل شناسایی‌شده در پالایش ترافیک VoIP وضعیت (حالت‌دار) (FFW_ACL_EXT.2.1) اجرا کند: أ. ترافیک SIP که در آن یک پیام BYE بر یک پیام INVITE اولویت دارد. ب. ترافیک H.225 که در آن یک پاسخ RCF مقدم بر هر ترافیک دیگری است. ت. ترافیک H.245 که در آن یک پیام پاسخ (ResponseMessage) مقدم بر پیام درخواست (RequestMessage) است. *[اختصاص: دیگر قوانین پالایش ترافیک وضعیت (حالت‌دار) پیش‌فرض]*	

۳۳	**پالایش ترافیک VoIP وضعیت (حالت‌دار) ۳**
محصول باید هر اتصالی که از قوانین پالایش ترافیک وضعیت (حالت‌دار) پیش‌فرض تخلف کرده است را خاتمه دهد و یک ثبت قابل ممیزی از رویداد تولید کند.	
۳۴	**پالایش ترافیک VoIP وضعیت (حالت‌دار) ۴**
محصول باید به‌صورت پویا پورت‌های رسانه را برای ترافیک پروتکل VoIP به‌محض تبادل با یک نشست باز کنند و به‌محض خاتمه یک نشست این پورت‌ها را ببندد.	
۳۵	**پالایش ترافیک VoIP وضعیت (حالت‌دار) ۵**
محصول نباید گستره ایستایی از پورت‌ها را تعریف کند که برای اجازه دادن به ترافیک پروتکل VoIP به‌طور نامحدودی باز بماند	
۳۶	**بازرسی عمیق بسته ۱**
محصول باید بازرسی عمیق بسته را برای پروتکل‌های: H:323، (H.225، H.245)، SIP، RTP، RTCP پیاده‌سازی کند.	
۳۷	**بازرسی عمیق بسته ۲**
محصول باید قوانین زیر را برای بازرسی بسته عمیق به کار گیرد: [*اختصاص: برای پروتکل‌های ذکرشده در بازرسی عمیق بسته (FFW_DPI_EXT.1.1)، عناصر داده بسته‌ای را فهرست کند که برای محتوای مخرب بالقوه و یا سازگاری با تعریف پروتکل موردبررسی* قرارگرفته است].	
۳۸	**بازرسی عمیق بسته ۳**
زمانی که تخلفی در یکی از قوانین بازرسی عمیق بسته در ترافیک یافت شود، محصول باید اقدامات زیر را انجام دهد: [انتخاب: رها کردن ترافیک، تولید یک ثبت ممیزی، تولید یک اخطار].	
۳۹	**پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۱**

محصول باید از برگردان نشانی شبکه[1] (NAT) ترافیک سیگنال دهی و کانال رسانه‌ای سرتاسر محصول پشتیبانی کند که عامل کاربر پشت‌به‌پشت STP تعریف‌شده در خط‌مشی کنترل جریان اطلاعات (FDP_IFC.1) در آن واسطه شده است.	
۴۰	**پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۲**
محصول باید از برگردان نشانی شبکه (NAT) برای پروتکل‌های زیر پشتیبانی کند [انتخاب: STP، H.225، H.245].	
۴۱	**پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۳**
محصول باید از برگردان نشانی شبکه (NAT) استفاده کند تا [انتخاب: نشانی IP محصول، یک مقدار تعریف‌شده مدیر سیستم امنیتی] را جایگزین مقادیر سربرگ نشانی IP از ترافیک آغازشده از شبکه داخلی کند.	
۴۲	**پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT) ۴**
محصول باید یک جدول برگردان نشانی شبکه (NAT) را حفظ کند تا اطمینان حاصل کند که محدوده ترافیک برای شبکه داخلی تنها معطوف به یک گیرنده داخلی است.	

۵-۲-۲-۵- کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۴۳	**سرور پروتکل آغاز نشست (SIP) ۱**
محصول باید پروتکل آغاز نشست (SIP) را مطابق با RFC 3261 پیاده‌سازی کنند. این پیاده‌سازی با استفاده از پروتکل توصیف نشست (SDP) مطابق با RFC 4566، برای توصیف نشست چندرسانه‌ای مورداستفاده برای انتقال ترافیک VoIP انجام می‌گیرد.	
۴۴	**سرور پروتکل آغاز نشست (SIP) ۲**

[1] Network Address Translation

محصول باید مستلزم احراز هویت کلمه عبور برای درخواست‌های تابع ثبت‌نام (REGISTER) پروتکل آغاز نشست (SIP) به نحو مشخص‌شده در بخش ۲۲ RFC 3261 باشد.	
سرور پروتکل آغاز نشست (SIP) ۳	۴۵
محصول باید مستلزم احراز هویت کلمه عبور برای درخواست‌های تابع ثبت‌نام (REGISTER) پروتکل آغاز نشست (SIP) به نحو مشخص‌شده در بخش ۲۲ RFC 3261 باشد.	
محصول باید از کلمه‌های عبور احراز هویت SIP پشتیبانی کند که حداقل شامل *[اختصاص: عدد صحیح مثبت ۸ رقمی یا بیشتر]* نویسه در مجموعه‌ای از *[نویسه‌های حروف کوچک، نویسه‌های حروف بزرگ، اعداد و نویسه‌های خاص: «!»، «@»، «#»، «&»، «*»، «(و)» و [اختصاص: دیگر نویسه‌های خاص پشتیبانی شده]]* باشد. **نکته کاربردی ۶:** تنها درخواست SIP ای لازم است (توسط محصول) احراز هویت شود که یک درخواست ثبت‌نام (REGISTER) باشد. سرور SIP اجرا را انجام داده و کاربر را تنها به‌محض ارائه کلمه عبور درست ثبت‌نام می‌کند؛ محصول برای پشتیبانی از کلمه‌های عبوری که دارای طول حداقل ۸ نویسه هستند (حداکثر طول در اولین اختصاص تعریف می‌شود) موردنیاز است و می‌تواند شامل نویسه‌های تعریف‌شده در سرور پروتکل آغاز نشست (FIA_SIPS_EXT.1.3) باشد (نویسه‌های مجاز توسط محصول که به‌صراحت در این عنصر ذکر نشده‌اند باید در اختصاص دوم شناسایی شوند، در غیر این صورت «هیچ نویسه دیگری» یک اختصاص قابل‌قبول خواهد بود.	
سرور پروتکل آغاز نشست (SIP) ۴	۴۶
محصول باید توانایی تغییر مقادیر سربرگ ترافیک SIP را قبل از انتقال مجدد ترافیک برای ترافیک SIP دریافت شده توسط محصول فراهم آورد.	
کانال دهی پروتکل آغاز نشست (SIP) ۱	۴۷
محصول باید پشتیبانی کانال دهی[۱] پروتکل آغاز نشست (SIP) را فراهم آورد.	
کانال دهی پروتکل آغاز نشست (SIP) ۲	۴۸

[۱] Trunking

این الزام وجود دارد که یک ارائه‌دهنده خدمت به‌منظور برقراری یک کانال SIP شناسایی معتبری را به شکل یک نام کاربری و نشانی IP برای محصول فراهم آورد.	
۴۹	**کانال دهی پروتکل آغاز نشست (SIP) ۳**
این الزام وجود دارد که یک ارائه‌دهنده خدمت به‌منظور برقراری یک کانال SIP اعتبارنامه احراز هویت معتبری را برای محصول فراهم آورد.	
۵۰	**کانال دهی پروتکل آغاز نشست (SIP) ۴**
این الزام وجود دارد که یک ارائه‌دهنده خدمت به‌منظور برقراری ارتباط با کانال SIP ترافیک را با استفاده از TLS و SRTP برای محصول رمزگذاری کند.	

۵-۲-۲-۶- کلاس اختصاص منابع (FRU)

شماره الزام	نام الزام
۵۱	**اولویت‌بندی محدود خدمت ۱**
محصول باید برای هر نوع بسته ارتباطی که از محصول عبور می‌کند اولویتی اختصاص دهد.	
۵۲	**اولویت‌بندی محدود خدمت ۲**
محصول باید اطمینان حاصل کند که هر دسترسی به [*پهنای باند شبکه*] باید بر اساس اولویت اختصاص داده‌شده به موجودیت فعال و فاکتور-R انجام‌گرفته باشد.	
۵۳	**حداکثر سهمیه‌ها ۱**
محصول باید حداکثر سهمیه از منابع زیر را اجرا کند: [واحد پردازنده مرکزی (CPU)، حافظه، *اختصاص: [منابع دیگر]* که [موجودیت‌های فعال] می‌توانند[انتخاب: به‌صورت هم‌زمان، در طی یک دوره مشخص از زمان] استفاده کنند. **نکته کاربردی ۷:** هدف از این الزام کارکرد امنیتی این است که محصول در مقابل حملات انکار خدمت مقاوم شود.	

۵-۲-۲-۷- کلاس کانال‌ها/مسیرهای مورد اعتماد

شماره الزام	نام الزام
۵۴	**کانال امن درون محصول ۱ (۲)**
محصول باید **قادر به استفاده از SIP-TLS، DTLS، SRTP، IPsec، H.235 [انتخاب: *[اختصاص: پروتکل‌های دیگر]*،هیچ پروتکل دیگری]** برای ارائه یک کانال امن بین خود و موجودیت‌های فناوری اطلاعات مجاز پشتیبانی‌کننده از قابلیت‌های زیر باشد: سیگنال دهی VoIP و کانال‌های رسانه‌ای که به‌طور منطقی از دیگر کانال‌های ارتباطی مجزا است و شناسایی امنی از نقاط پایانی‌اش و محافظت از داده کانال در برابر تغییر یا افشا را فراهم می‌آورد.	
۵۵	**کانال امن درون محصول ۲ (۲)**
محصول باید اجازه آغاز ارتباط را از طریق کانال امن به **محصول، یا موجودیت‌های مجاز فناوری اطلاعات** بدهد.	
۵۶	**کانال امن درون محصول ۳ (۲)**
محصول باید ارتباط از طریق کانال امن را برای *[اختصاص: فهرستی از توابع موردنیاز یک کانال امن]* آغاز کند. **نکته کاربردی ۸:** کانال امن درونی محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تکرار نشده است. نویسنده هدف امنیتی باید الزام کارکرد امنیتی تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را (همان‌گونه که در بخش ۵-۲-۱-۹ این بسته الحاقی پالایش‌شده است) به‌عنوان کانال امن درونی محصول ((FTP_ITC.1(1)) به‌گونه‌ای شناسایی کند که از قرارداد درست تکرار تبعیت شده باشد.	
۵۷	**کانال امن درون محصول ۱ (۳)**
محصول باید یک کانال **سیگنال دهی** بین خود و **سرور پروتکل آغاز نشست (SIP) با استفاده از پروتکل امنیت لایه انتقال (TLS) مشخص‌شده در پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت (FCS_TLSC_EXT.2) و [انتخاب: امنیت لایه انتقال دیتاگرام (DTLS) مشخص‌شده در امنیت لایه انتقال**	

دیتاگرام (FCS_DTLS_EXT.1)، هیچ پروتکل دیگری] ارائه دهد که به‌طور منطقی از دیگر کانال‌های ارتباطی مجزا است و شناسایی امنی از نقاط پایانی‌اش و محافظت از داده کانال در برابر تغییر یا افشا را فراهم می‌آورد	
کانال امن درون محصول ۲ (۳)	۵۸
محصول باید اجازه آغاز ارتباط را از طریق کانال امن به **محصول** بدهد.	
کانال امن درون محصول ۳ (۳)	۵۹
محصول باید ارتباط از طریق کانال امن را برای [*تمامی ارتباطات با سرور SIP*] آغاز کند. **نکته کاربردی ۹:** کانال امن درونی محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تکرار نشده است. نویسنده هدف امنیتی باید الزام کارکرد امنیتی تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را (همان‌گونه که در بخش ۵-۲-۱-۹ این بسته الحاقی پالایش‌شده است) به‌عنوان کانال امن درونی محصول ((FTP_ITC.1(1)) به‌گونه‌ای شناسایی کند که از قرارداد درست تکرار تبعیت شده باشد.	
کانال امن درون محصول ۱ (۴)	۶۰
محصول باید یک کانال ارتباطی **H.323** را **مطابق با ITU-REC H.235.0** بین خود و **نگهبان گیت[1] با استفاده از پروتکل امنیت لایه انتقال (TLS) مشخص‌شده در پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت (FCS_TLSC_EXT.2) و [انتخاب: امنیت پروتکل اینترنتی (IPsec) مشخص‌شده در امنیت پروتکل اینترنتی (FCS_IPSEC_EXT.1)، هیچ پروتکل دیگری]** ارائه دهد که به‌طور منطقی از دیگر کانال‌های ارتباطی مجزا است و شناسایی امنی از نقاط پایانی‌اش و محافظت از داده کانال در برابر تغییر یا افشا را فراهم می‌آورد.	
کانال امن درون محصول ۲ (۴)	۶۱

[1] gatekeeper

محصول باید اجازه آغاز ارتباط را از طریق کانال امن به **محصول** بدهد.	
۶۲	**کانال امن درون محصول ۳ (۴)**
محصول باید ارتباط از طریق کانال امن را برای [*تمامی ارتباطات با نگهبان گیت*] آغاز کند. **نکته کاربردی ۱۰:** کانال امن درونی محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تکرار نشده است. نویسنده هدف امنیتی باید الزام کارکرد امنیتی تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را (همان‌گونه که در بخش ۵-۲-۱-۹ این بسته الحاقی پالایش‌شده است) به‌عنوان کانال امن درونی محصول ((FTP_ITC.1(1)) به‌گونه‌ای شناسایی کند که از قراردادهای درست تکرار تبعیت شده باشد	

۶- اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی

در این بخش، اقدامات تضمینی که ارزیاب مبتنی بر الزامات کارکرد امنیتی محصول و پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) باید انجام دهد، برای هر الزام به‌طور جداگانه در جداولی ارائه‌شده است.

۶-۱- اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)

جدول ۳ اقدامات تضمین الزام تولید داده ممیزی

اقدامات تضمین الزام کارکرد امنیتی تولید داده ممیزی
ارزیاب باید برای تولید داده ممیزی (FAU_GEN.1) اقدام تضمین را همان‌گونه انجام دهد که در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) برای رویدادهای قابل ممیزی تعریف‌شده در بالا، علاوه بر رویدادهای ممیزی کاربردپذیر تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) توصیف‌شده است. ارزیاب باید مطمئن شود که اقدامات اداری تعریف‌شده برای این بسته الحاقی به‌صورت مناسب مورد ممیزی قرارگرفته‌اند.

جدول ۴ اقدامات تضمین الزام امنیتی عملیات رمزنگاری (رمزگذاری/ رمزگشایی داده استاندارد رمزگذاری پیشرفته)

اقدام تضمین الزام کارکرد امنیتی عملیات رمزنگاری (رمزگذاری/ رمزگشایی داده استاندارد رمزگذاری پیشرفته)
هیچ آزمون اضافی برای این الزام کارکرد امنیتی موردنیاز نیست مگر اینکه پیاده‌سازی استاندارد رمزگذاری پیشرفته (AES) مورداستفاده توسط قابلیت کارکردی کنترل‌کننده محدوده نشست (SBC) محصول، از یک پیاده‌سازی الگوریتم رمزنگاری متفاوت استفاده کند. در این صورت، ارزیاب باید اقدام تضمین تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) برای این الزام کارکرد امنیتی را جهت پیاده‌سازی الگوریتم جدید تکرار کند.

جدول ۵ اقدام تضمین الزام امنیت پروتکلی

اقدام تضمین الزام کارکرد امنیتی امنیت پروتکلی
هیچ آزمون اضافی فراتر از آنچه برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) موردنیاز است، برای این الزام کارکرد امنیتی نیاز نیست.

جدول ۶ اقدام تضمین الزام پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت

اقدام تضمین الزام کارکرد امنیتی پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت
هیچ آزمون اضافی فراتر از آنچه برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) موردنیاز است، برای این الزام کارکرد امنیتی نیاز نیست.

جدول ۷ اقدامات تضمین الزام پروتکل سرویس‌دهنده امنیت لایه انتقال با احراز هویت

اقدام تضمین الزام کارکرد امنیتی پروتکل سرویس‌دهنده امنیت لایه انتقال با احراز هویت
هیچ آزمون اضافی‌ای فراتر از آنچه برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) موردنیاز است، برای این الزام کارکرد امنیتی نیاز نیست.

جدول ۸ اقدام تضمین الزام کارکرد امنیتی مشخصات توابع مدیریت

اقدام تضمین الزام کارکرد امنیتی مشخصات توابع مدیریت
انطباق با الزامات کارکرد امنیتی در بخش ۵-۲-۲ این بسته الحاقی برای نشان دادن این موضوع که محصول ابزارهای کافی برای مدیریت توابع کنترل‌کننده محدوده نشست (SBC) خود فراهم آورده است، کافی است.

جدول ۹ اقدام تضمین الزام پالایش مهرهای زمانی مطمئن ۱

اقدام تضمین الزام کارکرد امنیتی پالایش مهرهای زمانی مطمئن ۱	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول (TSS) توانایی محصول برای پشتیبانی از هم‌زمان‌سازی پروتکل زمانی شبکه (NTP) را توضیح داده باشد.
AGD	ارزیاب باید مستندات راهنما را مورد بازبینی قرار دهد تا تائید کند که این اسناد دستورالعمل‌هایی در مورد نحوه ایجاد توانایی برای هم‌زمان‌سازی NTP ارائه می‌دهند.

TEST	ارزیاب باید به‌صورت دستی زمان سامانه را روی یک مقدار نادرست تنظیم کند. سپس مستندات راهنما را دنبال کند تا هم‌زمان‌سازی NTP را فعال کند، با یک سرور NTP هم‌زمان‌سازی را انجام داده و مشاهده کند که زمان سامانه به زمان جاری تنظیم‌شده است.

جدول ۱۰ اقدام تضمین الزام کانال امن درون محصول

اقدام تضمین الزام کارکرد امنیتی کانال امن درون محصول
این الزام کارکرد امنیتی پالایشی از کانال امن درون محصول (FTP_ITC.1) تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) است. ارزیاب باید همان اقدامات تضمین تعریف‌شده برای کانال امن درون محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را برای این الزام کارکرد امنیتی اصلاح (پالایش) شده تکرار کند.

۶-۲- اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی محصول

جدول ۱۱ اقدامات تضمین الزام هشدارهای امنیتی ۱

اقدام تضمین الزام کارکرد امنیتی هشدارهای امنیتی ۱	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول (TSS) توانایی محصول را برای انتقال تخلف‌های امنیتی بالقوه به یک گیرنده دریچه به دریچه SNMPv3 توضیح می‌دهد.
AGD	ارزیاب باید بررسی کند که راهنمای هدایت عملیاتی، دستورالعمل‌هایی در مورد نحوه پیکربندی محصول ارائه می‌دهد تا محصول قادر به مخابره کردن تخلف‌های امنیتی بالقوه به یک گیرنده دریچه به دریچه SNMPv3 باشد.
TEST	ارزیاب باید محصول را در محیطی قرار دهد که شامل یک گیرنده دریچه به دریچه SNMPv3 است. وی باید محصول را جهت برقراری ارتباط با گیرنده به شیوه مشخص‌شده توسط مستندات راهنما (AGD) پیکربندی کند. ارزیاب باید ابزار ضبط بسته‌ای[۱] را به کار گیرد که قادر به ردیابی ترافیک بین گیرنده و محصول باشد. برای هر نوع تخلف امنیتی بالقوه که توسط هدف امنیتی تعریف‌شده است، ارزیاب باید موجب شود که آن تخلف امنیتی بالقوه در محصول رخ دهد و اگر لازم باشد که محصول رفتاری را به‌عنوان یک تخلف امنیتی بالقوه تشخیص دهد باید محصول را برای انجام چنین کاری پیکربندی کند.

[۱] Packet capture tools [**Packet capture** is the process of intercepting and logging traffic]

	بسته به آن چیزی که محصول به‌عنوان تخلف بالقوه امنیتی در نظر می‌گیرد، ممکن است لازم باشد ارزیاب، تولیدکنندگان ترافیک، سلاح‌های گرم و یا دیگر تجهیزات مورداستفاده برای شبیه‌سازی تخلف‌های امنیتی بالقوه را تنظیم و راه‌اندازی کند. پس از این کار، ارزیاب باید با استفاده از ابزار ضبط بسته و تعامل مستقیم با گیرنده مشاهده کند که محصول، تخلف امنیتی بالقوه را انتقال داده و به‌درستی از پروتکل SNMPv3 استفاده کرده است.

جدول ۱۲ اقدامات تضمین الزام تحلیل تخلف بالقوه

اقدام تضمین الزام کارکرد امنیتی تحلیل تخلف بالقوه	
TSS	ارزیاب باید بررسی کند که آیا خلاصه مشخصات محصول شرایطی را تشریح می‌کند که محصول آن را به‌عنوان تخلف امنیتی بالقوه نشانه‌گذاری می‌کند و آیا این شرایط به‌صورت اجرایی قابل پیکربندی هستند یا خیر.
AGD	اگر شرایط توسط محصول به‌عنوان تخلف امنیتی قابل پیکربندی پرچم‌دار شده باشد، ارزیاب باید راهنماهای عملیاتی را بررسی کند تا تعیین کند که این راهنماها توضیح دهد که چگونه یک مدیر سیستم می‌تواند تخلف‌های امنیتی بالقوه را پیکربندی کند.
Test	آزمون این الزام کارکرد امنیتی همراه با هشدارهای امنیتی (FAU_ARP.1) تکمیل‌شده است. این الزام کارکرد امنیتی با ایجاد هر نوع تخلف امنیتی بالقوه تعریف‌شده توسط محصول و مشاهده این‌که با این تخلف‌های امنیتی بالقوه به‌درستی و همان‌گونه که باید، رفتار می‌شوند مورد آزمون قرار خواهد گرفت. این فعالیت به‌عنوان قسمتی از اقدامات تضمین برای هشدارهای امنیتی (FAU_ARP.1) انجام‌شده است، بنابراین آزمون جداگانه‌ای موردنیاز نیست.

جدول ۱۳ اقدامات تضمین الزام امنیت لایه انتقال دیتاگرام

اقدامات تضمین الزام کارکرد امنیتی امنیت لایه انتقال دیتاگرام	
به یاد داشته باشید که این اقدام تضمین دربرگیرنده همان روش‌های اجرایی مشخص‌شده توسط پروتکل سرویس‌گیرنده امنیت لایه انتقال با احراز هویت (FCS_TLSC_EXT.2) است که در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تعریف‌شده‌اند، به‌جز مواردی که برای پیاده‌سازی پروتکل امنیت لایه انتقال دیتاگرام (DTLS) محصول به کار گرفته می‌شوند.	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول را برای استفاده از پروتکل امنیت لایه انتقال دیتاگرام (DTLS) را توضیح داده و شرح می‌دهد که چه دنباله رمزهایی با پیاده‌سازی پروتکل امنیت لایه انتقال دیتاگرام (DTLS) پشتیبانی می‌شوند.
AGD	چنانچه هر جنبه‌ای از پیاده‌سازی پروتکل امنیت لایه انتقال دیتاگرام (DTLS) به پیکربندی نیاز داشته باشد، ارزیاب باید تائید کند که روش انجام این کار در مستندات راهنما تشریح شده است.

Test	ارزیاب باید آزمون زیر را انجام دهد: ۱- در صورت لزوم، پیکربندی محصول برای استفاده از پروتکل امنیت لایه انتقال دیتاگرام (DTLS). ۲- استقرار یک ابزار ضبط بسته که قادر به ردیابی ترافیک بر روی رابط‌های شبکه‌ای باشد که در آن ترافیک امنیت لایه انتقال دیتاگرام (DTLS) انتقال داده خواهد شد. ۳- برقراری یک اتصال پروتکل امنیت لایه انتقال دیتاگرام (DTLS) با محصول و تائید این موضوع که با استفاده از ابزارهای ضبط بسته و ثبت وقایع ممیزی، ارتباطات پروتکل امنیت لایه انتقال دیتاگرام (DTLS) برقرارشده‌اند و ترافیک رمزگذاری شده بر روی کانال پروتکل امنیت لایه انتقال دیتاگرام (DTLS) انتقال‌یافته است. ۴- تکرار این آزمون برای هر دنباله رمز پشتیبانی شده در پیاده‌سازی پروتکل امنیت لایه انتقال دیتاگرام (DTLS)

جدول ۱۴ اقدام تضمین الزام پروتکل انتقال بلادرنگ

اقدام تضمین الزام کارکرد امنیتی پروتکل انتقال بلادرنگ	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول برای انجام موارد زیر توضیح می‌دهد: ۱- پشتیبانی از استفاده از پروتکل انتقال بلادرنگ امن (SRTP) و دنباله رمزهایی که با پیاده‌سازی پروتکل انتقال بلادرنگ امن (SRTP) پشتیبانی می‌شوند. ۲- فراهم آوردن توانایی غیرفعال کردن الگوریتم SRTP NULL برای مدیر سیستم امنیتی. ۳- فراهم آوردن توانایی مشخص کردن پورت‌های پروتکل انتقال بلادرنگ امن (SRTP) مورداستفاده در ارتباطات پروتکل انتقال بلادرنگ امن (SRTP) برای مدیر سیستم امنیتی.
AGD	ارزیاب باید بررسی کند که راهنمای عملیاتی نحوه‌ی انجام اقدامات زیر را بر روی محصول توضیح دهد: ۱- چگونگی پیکربندی دنباله رمزهای مورداستفاده شده توسط پروتکل انتقال بلادرنگ امن (SRTP) ۲- چگونگی فعال یا غیرفعال کردن استفاده از الگوریتم SRTP NULL ۳- چگونگی مشخص کردن پورت‌های مورداستفاده برای ارتباطات پروتکل انتقال بلادرنگ امن (SRTP)
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** ۱- در صورت لزوم، پیکربندی محصول برای استفاده از پروتکل انتقال بلادرنگ امن (SRTP).

۲- استقرار یک ابزار ضبط بسته که قادر به ردیابی ترافیک بر روی رابط شبکه‌ای باشد که در آن ترافیک امنیت لایه انتقال دیتاگرام (DTLS) انتقال داده خواهد شد. ۳- برقراری یک اتصال پروتکل امنیت لایه انتقال دیتاگرام (DTLS) با محصول و تائید این موضوع که با استفاده از ابزارهای ضبط بسته و ثبت وقایع ممیزی، ارتباطات پروتکل امنیت لایه انتقال دیتاگرام (DTLS) برقرارشده‌اند و ترافیک رمزگذاری شده بر روی کانال پروتکل امنیت لایه انتقال دیتاگرام (DTLS) انتقال‌یافته است. ۴- تکرار این آزمون برای هر مجموعه رمزنگاری جهت پشتیبانی از اجرای پروتکل انتقال بلادرنگ امن (SRTP) **آزمون ۲:** ۱- پیکربندی محصول جهت فعال کردن با استفاده از الگوریتم SRTP NULL ۲- استقرار یک ابزار ضبط بسته که قادر به ردیابی ترافیک بر روی رابط شبکه‌ای باشد که در آن ترافیک امنیت لایه انتقال دیتاگرام (DTLS) انتقال داده خواهد شد. ۳- انتقال پیام SRTP NULL به محصول و مشاهده این‌که محصول آن را پذیرفته است. ۴- پیکربندی محصول جهت غیرفعال کردن استفاده از الگوریتم SRTP NULL ۵- انتقال پیام SRTP NULL به محصول و مشاهده این‌که محصول آن را رد کرده است. **آزمون ۳:** ۱- پیکربندی محصول برای استفاده از پورت مشخص‌شده برای ترافیک پروتکل انتقال بلادرنگ امن (SRTP). ۲- استقرار یک ابزار ضبط بسته که قادر به ردیابی ترافیک بر روی رابط شبکه‌ای باشد که در آن ترافیک امنیت لایه انتقال دیتاگرام (DTLS) انتقال داده خواهد شد. ۳- انتقال ترافیک پروتکل انتقال بلادرنگ امن (SRTP) به محصول و مشاهده این‌که ترافیک بر روی پورت مشخص‌شده انتقال می‌یابد. ۴- پیکربندی محصول برای استفاده از یک پورت متفاوت برای ترافیک پروتکل انتقال بلادرنگ امن (SRTP) ۵- انتقال ترافیک پروتکل انتقال بلادرنگ امن (SRTP) به محصول و مشاهده این‌که ترافیک بر روی پورت جدیداً مشخص‌شده انتقال می‌یابد.	

جدول ۱۵ اقدام تضمین الزام خط‌مشی کنترل جریان اطلاعات ۱

اقدام تضمین الزام کارکرد امنیتی خط‌مشی کنترل جریان اطلاعات ۱	
TSS	N/A - آزمون این الزام کارکرد امنیتی به‌عنوان قسمتی از توابع کنترل جریان اطلاعات (FDP_IFF.1) انجام‌شده است.
AGD	N/A - آزمون این الزام کارکرد امنیتی به‌عنوان قسمتی از توابع کنترل جریان اطلاعات (FDP_IFF.1) انجام‌شده است.
Test	N/A - آزمون این الزام کارکرد امنیتی به‌عنوان قسمتی از توابع کنترل جریان اطلاعات (FDP_IFF.1) انجام‌شده است.

جدول ۱۶ اقدام تضمین الزام توابع کنترل جریان اطلاعات

اقدام تضمین الزام کارکرد امنیتی توابع کنترل جریان اطلاعات	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول را برای عملکرد به‌عنوان یک عامل B2BUA شرح داده و توانایی عملکرد در هر دو حالت فهرست سیاه یا فهرست سفید را ارائه داده است.
AGD	ارزیاب باید راهنمای عملیاتی را مورد بازبینی قرار دهد تا بررسی کند که دستورالعمل‌هایی را برای تنظیم محصول در یک حالت فهرست سیاه یا سفید ارائه داده و چگونگی افزودن یا حذف موجودیت‌ها از فهرست سیاه و فهرست سفید را شرح داده است.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** یک فهرست کنترل دسترسی (ACL) سفارشی را برای رد یک تماس آغازشده از یک نشانی IP یا زیرشبکه پیکربندی کرده، تماسی از آن نشانی IP یا زیرشبکه گرفته شود و تائید شود که تماس نمی‌تواند کامل شود. بررسی شود که تماس از هر نشانی IP و یا زیرشبکه دیگری یک تماس کامل خواهد بود. **آزمون ۲:** یک فهرست کنترل دسترسی (ACL) سفارشی را برای اجازه دادن به تنها یک تماس آغازشده از یک نشانی IP یا زیرشبکه پیکربندی کرده، تماسی از آن نشانی IP یا زیرشبکه گرفته شود و تائید شود که تماس می‌تواند کامل شود. **آزمون ۳:**

یک فهرست کنترل دسترسی (ACL) سفارشی را برای رد یک تماس به مقصد یک نشانی IP یا زیرشبکه پیکربندی کرده، تماسی از آن نشانی IP یا زیرشبکه گرفته شود و تائید شود که تماس نمی‌تواند کامل شود. بررسی شود که تماس به هر نشانی IP و یا زیرشبکه دیگری یک تماس کامل خواهد بود. **آزمون ۴:** یک فهرست کنترل دسترسی (ACL) سفارشی را برای اجازه دادن به تنها یک تماس به مقصد یک نشانی IP یا زیرشبکه پیکربندی کرده، تماسی از آن نشانی IP یا زیرشبکه گرفته شود و تائید شود که تماس می‌تواند کامل شود. بررسی شود که تماس به هر نشانی IP و یا زیرشبکه دیگری یک تماس کامل نخواهد بود. **آزمون ۵:** یک فهرست کنترل دسترسی (ACL) سفارشی را برای رد یک تماس با استفاده از پروتکل سیگنال دهی (مانند SIP) و یا پروتکل رسانه (مانند RTP) معین پیکربندی کرده، تماسی با استفاده از آن پروتکل گرفته شود و تائید شود که تماس نمی‌تواند کامل شود. بررسی شود که تماس‌های استفاده‌کننده از دیگر پروتکل‌های سیگنال دهی (مانند H.323) و یا پروتکل‌های رسانه (مانند SRPT) یک تماس کامل خواهد بود. **آزمون ۶:** یک فهرست کنترل دسترسی (ACL) سفارشی را برای اجازه دادن به تنها یک تماس استفاده‌کننده از پروتکل سیگنال دهی (مانند SIP) و یا پروتکل رسانه (مانند RTP) معین پیکربندی کرده، تماسی با استفاده از آن پروتکل گرفته شود و تائید شود که تماس می‌تواند کامل شود. بررسی شود که تماس‌های استفاده‌کننده از دیگر پروتکل‌های سیگنال دهی (مانند H.323) و یا پروتکل‌های رسانه (مانند SRPT) یک تماس کامل نخواهد بود. **آزمون ۷:** در محصول، فهرست سفیدی از تماس‌گیرندگان مجاز پیکربندی‌شده و شماره‌های دیگر مسدود شوند. پیکربندی را از طریق ثبت وقایع ممیزی تائید کرده، تماسی از طریق محصول از هر یک از اعداد موجود در فهرست سفید برقرار شود. بررسی شود که هر شماره می‌تواند تماس کاملی را برقرار کند. تلاش شود تا تماسی از طریق محصول از دیگر اعدادی که در فهرست سفید نیستند برقرار شود و بررسی شود که آن تماس‌ها نمی‌توانند کامل شوند. **آزمون ۸:** در محصول، فهرست سفیدی از تماس‌گیرندگان مجاز با نشانی IP پیکربندی‌شده و نشانی‌های IP دیگر مسدود شوند. پیکربندی را از طریق ثبت وقایع ممیزی تائید کرده، تماسی از طریق محصول از هر یک از نشانی IP موجود در فهرست سفید برقرار شود. بررسی شود که هر نشانی IP می‌تواند تماس کاملی را برقرار کند. نشانی IP	

	نقاط پایانی را تغییر داده؛ با این حال، همان شماره‌های تماس حفظ شود. تلاش شود تا تماسی از طریق محصول از نشانی IP جدیدی برقرار شود و بررسی شود که آن تماس‌ها نمی‌توانند کامل شوند. **آزمون ۹:** در محصول، فهرست سیاهی از تماس‌گیرندگان غیرمجاز با شماره تماس پیکربندی‌شده و شماره‌های تماس دیگر مجاز باشند. پیکربندی را از طریق ثبت وقایع ممیزی تائید کرده، تلاش شود تا تماسی از طریق محصول از هر یک از شماره‌های موجود در فهرست سیاه برقرار شود. بررسی شود که هیچ‌یک از شماره‌ها نمی‌تواند تماس کاملی را برقرار کند. تماسی از طریق محصول از دیگر شماره‌هایی که در فهرست سیاه وجود ندارد برقرار کرده و بررسی شود که آن تماس‌ها می‌توانند کامل شوند. **آزمون ۱۰:** در محصول، فهرست سیاهی از تماس‌گیرندگان غیرمجاز با نشانی IP پیکربندی‌شده و دیگر نشانی IP مجاز باشند. پیکربندی را از طریق ثبت وقایع ممیزی تائید کرده، تلاش شود تا تماسی از طریق محصول از هر یک از نشانی‌های IP موجود در فهرست سیاه برقرار شود. بررسی شود که هیچ‌یک نشانی IP نمی‌تواند تماس کاملی را برقرار کند. نشانی IP نقاط پایانی را تغییر داده؛ با این حال، همان شماره‌های تماس حفظ شود. تلاش شود تا تماسی از طریق محصول از نشانی IP جدیدی برقرار شود و بررسی شود که آن تماس‌ها می‌توانند کامل شوند.

جدول ۱۷ اقدام تضمین الزام پالایش ترافیک VoIP 1

اقدام تضمین الزام کارکرد امنیتی پالایش ترافیک VoIP 1	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول شرحی از فرایند راه‌اندازی یا مقداردهی اولیه محصول را ارائه می‌دهد که به‌وضوح نشان می‌دهد که در کجا پردازش بسته‌های شبکه شروع شده و استدلالی را ارائه می‌دهد که این ادعا را پشتیبانی می‌کند که بسته‌ها نمی‌توانند در طول این فرایند جریان داشته باشند. ارزیاب باید بررسی کند که خلاصه مشخصه محصول شرحی را شامل می‌شود که مؤلفه‌های درگیر در پردازش بسته‌های شبکه (مانند موجودیت‌های فعال از قبیل یک فرایند یا وظیفه) را شناسایی کرده و محافظ‌های امنی را توصیف می‌کند که از جریان بسته‌ها در سرتاسر محصول محافظت می‌کند بدون آنکه مجموعه قوانینی را در صورت شکست مؤلفه اعمال کند. این شکست می‌تواند شامل شکست یک مؤلفه، مثل فرآیند خاتمه یافته و یا شکست درون یک مؤلفه مانند پر شدن بافرهای حافظه و عدم توانایی در پردازش بسته‌ها باشد.
AGD	مستندات راهنمای مرتبط با این الزام در فعالیت‌های تضمین آزمون متعاقب ارزیابی خواهد شد.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد:

	آزمون ۱: درحالی‌که محصول در حال مقداردهی شدن است، ارزیاب باید برای به دست آوردن ترافیک شبکه برای جریان از طریق محصول تلاش کند. یک جریان ثابت از بسته‌های شبکه که ممکن است با مجموعه قوانین دیگر رد شود باید به یک میزبان منبع یابی و هدایت شود. ارزیاب باید با استفاده از یک بسته ردیاب بررسی کند که هیچ ترافیک شبکه تولیدشده‌ای از طریق دیواره آتش در طول مقداردهی اولیه مجاز نشده است. **آزمون ۲:** درحالی‌که محصول در حال مقداردهی شدن است، ارزیاب باید برای به دست آوردن ترافیک شبکه برای جریان از طریق محصول تلاش کند. یک جریان ثابت از بسته‌های شبکه که ممکن است با مجموعه قوانین دیگر مجاز شناخته شود باید به یک میزبان منبع یابی و هدایت شود. ارزیاب باید با استفاده از یک بسته ردیاب بررسی کند که هیچ ترافیک شبکه تولیدشده‌ای از طریق دیواره آتش در طول مقداردهی اولیه مجاز نشده است و تنها زمانی اجازه یافتند که مقداردهی اولیه کامل شده است.

جدول ۱۸ اقدام تضمین الزام پالایش ترافیک VoIP ۴

اقدام تضمین الزام کارکرد امنیتی پالایش ترافیک VoIP۴	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول خط‌مشی پالایش بسته را شرح داده و خصیصه‌های زیر را در درون قوانین پالایش ترافیک برای پروتکل‌های مرتبط قابل پیکربندی می‌دانند: • ICMPv4 ○ نوع ○ کد • ICMPv6 ○ نوع ○ کد • IPv4

	○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال • IPv6 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال و در جایی که نویسنده هدف امنیتی تعریف کرد، نوع سربرگ بسط یافته، رشته‌های (فیلدهای) سربرگ بسط یافته • TCP ○ پورت منبع ○ پورت مقصد • UDP ○ پورت منبع ○ پورت مقصد ارزیاب باید بررسی کند که هر قانون می‌تواند اقدامات زیر را شناسایی کند: اجازه دادن و یا رها کردن با گزینه انتخابی برای ثبت عملیات. ارزیاب باید بررسی کند که خلاصه مشخصه محصول تمام انواع رابط‌هایی که مشمول خط‌مشی پالایش بسته می‌باشند را شناسایی کرده و توضیح می‌دهد که چگونه قوانین به رابط‌های مجزای شبکه مرتبط می‌شوند.
AGD	ارزیاب باید بررسی کند که مستندات راهنما خصیصه‌های زیر را در درون قوانین پالایش ترافیک برای پروتکل‌های مرتبط قابل پیکربندی می‌دانند: • ICMPv4 ○ نوع ○ کد • ICMPv6

	○ نوع ○ کد • IPv4 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال • IPv6 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال و در جایی که نویسنده هدف امنیتی تعریف کرد، نوع سربرگ بسط یافته، رشته‌های (فیلدهای) سربرگ بسط یافته • TCP ○ پورت منبع ○ پورت مقصد • UDP ○ پورت منبع ○ پورت مقصد ارزیاب باید بررسی کند که مستندات راهنما نشان می‌دهد که هر قانون می‌تواند اقدامات زیر را شناسایی کند: اجازه دادن و یا رها کردن و ثبت وقایع. ارزیاب باید بررسی کند که مستندات راهنما توضیح می‌دهد که چگونه قوانین به رابط‌های شبکه مجزا مرتبط می‌شوند.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:**

	ارزیاب باید از دستورالعمل‌های موجود در مستندات راهنما استفاده کند تا این موضوع را مورد آزمون قرار دهد که قوانین دیواره آتش پالایش بسته وضعیت (حالت‌داری) را می‌توان ایجاد کرد که برای هر یک از خصیصه‌های زیر امکان اجازه دادن، رها کردن و ثبت کردن به بسته‌ها را بدهد: • ICMPv4 ○ نوع ○ کد • ICMPv6 ○ نوع ○ کد • IPv4 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال • IPv6 ○ نشانی منبع ○ نشانی مقصد ○ پروتکل لایه انتقال و در جایی که نویسنده هدف امنیتی تعریف کرد، نوع سربرگ بسط یافته، رشته‌های (فیلدهای) سربرگ بسط یافته • TCP ○ پورت منبع ○ پورت مقصد • UDP ○ پورت منبع

	○ پورت مقصد **آزمون ۲:** اقدام تضمین آزمون بالا باید تکرار شود تا اطمینان حاصل شود که قوانین پالایش ترافیک را می‌توان برای هر نوع رابط شبکه مجزا پشتیبانی شده توسط محصول تعریف نمود.

جدول ۱۹ اقدام تضمین الزام پالایش ترافیک VoIP5

اقدام تضمین الزام کارکرد امنیتی پالایش ترافیک VoIP 5	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول پروتکل‌های پشتیبانی‌کننده از ساماندهی نشست را شناسایی می‌کند. خلاصه مشخصه محصول باید TCP، UDP و ICMP را درصورتی‌که توسط نویسنده هدف امنیتی انتخاب شود شناسایی کند. ارزیاب باید بررسی کند که خلاصه مشخصه محصول توضیح می‌دهد که چگونه نشست‌ها برقرارشده (از جمله پردازش دست‌داد) و حفظ و نگهداری می‌شود. ارزیاب باید بررسی کند که خلاصه مشخصه محصول استفاده از خصیصه‌های زیر را در تعیین نشست برای TCP شناسایی کرده و توضیح می‌دهد: نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد، اعداد دنباله و پرچم‌های منحصربه‌فرد. ارزیاب باید بررسی کند که خلاصه مشخصه محصول خصیصه‌های زیر را در تعیین نشست برای UDP شناسایی کرده و توضیح می‌دهد: نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد. ارزیاب باید بررسی کند که خلاصه مشخصه محصول خصیصه‌های زیر را در تعیین نشست برای ICMP (درصورتی‌که انتخاب شود) شناسایی کرده و توضیح می‌دهد: نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد، دیگر خصیصه‌های انتخاب‌شده در پالایش ترافیک VoIP (FFW_ACL_EXT.1.5). ارزیاب باید بررسی کند که خلاصه مشخصه محصول توضیح دهد که چگونه نشست‌های برقرارشده حذف‌شده‌اند. خلاصه مشخصه محصول باید توضیح دهد که چگونه اتصالات هر پروتکل بر اساس شرایط تکمیل نرمال و یا وقفه حذف‌شده‌اند. علاوه بر آن خلاصه مشخصه محصول باید نشان دهد که چه زمانی حذف نشست اثربخش خواهد بود (به‌عنوان مثال، قبل از اینکه بسته بعدی انطباق یابد، نشست پردازش‌شده است).
AGD	ارزیاب باید بررسی کند که مستندات راهنما رفتارهای نشست را توضیح می‌دهد. به‌عنوان مثال محصول ممکن است بسته‌هایی که به‌عنوان قسمتی از یک نشست موجود مجاز شده‌اند را ثبت نکند.

Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** ارزیاب باید محصول را برای اجازه و ثبت ترافیک TCP پیکربندی کند. ارزیاب باید یک نشست TCP را شروع کند. درحالی‌که نشست TCP برقرارشده است، ارزیاب باید بسته‌های برقراری نشست را با پرچم‌های نادرست معرفی کند تا تعیین شود که ترافیک تغییریافته به‌عنوان قسمتی از نشست پذیرفته‌نشده است (به‌عنوان مثال یک رویداد ثبت تولیدشده است تا نشان دهد که مجموعه قوانین به کار گرفته‌شده است). بعد از برقراری موفق نشست TCP، ارزیاب باید هر یک از خصیصه‌های تعیین‌کننده نشست (نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد، اعداد دنباله و پرچم‌ها) را یک‌بار تغییر دهد تا بررسی کند که بسته‌های تغییریافته به‌عنوان قسمتی از نشست برقرارشده پذیرفته‌نشده است. **آزمون ۲:** ارزیاب باید نشست TCP برقرارشده برای آزمون ۱ را همان‌گونه که در خلاصه مشخصه محصول توضیح داده‌شده است، خاتمه دهد. سپس ارزیاب باید بلافاصله یک بسته مطابق نشست قبلی ارسال کند تا اطمینان یابد که این بسته از طریق محصول بدون اینکه مشمول مجموعه قوانین باشد فرستاده نشده است. **آزمون ۳:** ارزیاب باید نشست TCP برقرارشده برای آزمون ۱ را همان‌گونه که در خلاصه مشخصه محصول توضیح داده‌شده است، منقضی کند (به‌عنوان مثال رسیدن به یک وقفه). سپس ارزیاب باید بلافاصله یک بسته مطابق نشست قبلی ارسال کند تا اطمینان یابد که این بسته از طریق محصول بدون اینکه مشمول مجموعه قوانین باشد فرستاده نشده است. **آزمون ۴:** ارزیاب باید محصول را برای اجازه و ثبت ترافیک UDP پیکربندی کند. ارزیاب باید یک نشست UDP برقرار کند. هنگامی که نشست UDP برقرار شد، ارزیاب باید هر یک از خصیصه‌های تعیین‌کننده نشست (نشانی‌های منبع و مقصد، پورت‌های منبع و مقصد) را یک‌بار تغییر دهد تا بررسی کند که بسته‌های تغییریافته به‌عنوان قسمتی از نشست برقرارشده پذیرفته‌نشده است. **آزمون ۵:**

ارزیاب باید نشست UDP برقرارشده برای آزمون ۴ را همان‌گونه که در خلاصه مشخصه محصول توضیح داده‌شده است، منقضی کند (به‌عنوان مثال رسیدن به یک وقفه). سپس ارزیاب باید یک بسته مطابق نشست قبلی ارسال کند تا اطمینان یابد که این بسته از طریق محصول بدون اینکه مشمول مجموعه قوانین باشد فرستاده نشده است. **آزمون ۶:** اگر ICMP انتخاب‌شده باشد، ارزیاب باید محصول را برای اجازه و ثبت ترافیک ICMP پیکربندی کند. ارزیاب باید یک نشست برای ICMP را همان‌گونه که در خلاصه مشخصه محصول تعریف‌شده است برقرار کند. هنگامی که نشست ICMP برقرار شد، ارزیاب باید هر یک از خصیصه‌های تعیین‌کننده نشست (نشانی‌های منبع و مقصد، دیگر خصیصه‌های انتخاب‌شده در پالایش ترافیک VoIP (FFW_ACL_EXT.1.5)) را یک‌بار تغییر دهد تا بررسی کند که بسته‌های تغییریافته به‌عنوان قسمتی از نشست برقرارشده پذیرفته‌نشده است. **آزمون ۷:** در صورت امکان، ارزیاب باید نشست برقرارشده ICMP برای آزمون ۶ را به نحوی که در خلاصه مشخصه محصول توصیف‌شده است، خاتمه دهد. سپس ارزیاب باید بلافاصله یک بسته مطابق تعریف نشست قبلی ارسال کند تا اطمینان یابد که این بسته از طریق محصول بدون اینکه مشمول مجموعه قوانین باشد فرستاده نشده است. **آزمون ۸:** ارزیاب باید نشست برقرارشده ICMP برای آزمون ۶ را به نحوی که در خلاصه مشخصه محصول توصیف‌شده است، منقضی کند (به‌عنوان مثال رسیدن به یک وقفه). سپس ارزیاب باید یک بسته مطابق نشست قبلی ارسال کند تا اطمینان یابد که این بسته از طریق محصول بدون اینکه مشمول مجموعه قوانین باشد فرستاده نشده است.	

جدول ۲۰ اقدام تضمین الزام پالایش ترافیک VoIP۶

اقدام تضمین الزام کارکرد امنیتی پالایش ترافیک VoIP 6	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول الگوریتم اعمال‌شده برای بسته‌های ورودی را توصیف کند، از جمله پردازش قوانین پیش‌فرض، تعیین اینکه آیا بسته قسمتی از یک نشست برقرارشده است یا خیر و کاربرد مدیر سیستم تعریف‌شده و مجموعه قوانین ترتیب داده‌شده.
AGD	ارزیاب باید بررسی کند که مستندات راهنما توضیح می‌دهد که چگونه ترتیب قوانین پالایش ترافیک تعیین‌شده است و دستورالعمل‌های ضروری را به‌گونه‌ای فراهم آورد که یک مدیر سیستم بتواند ترتیب پردازش قوانین را پیکربندی کند.
Test	ارزیاب باید این آزمون‌ها را انجام دهد: **آزمون ۱:** ارزیاب باید دو قانون پالایش ترافیک با وضعیت کاملاً مساوی را با عملیات تبادل –اجازه دادن و رها کردن در نظر بگیرد. قوانین باید در دو ترتیب مجزا گسترش‌یافته و در هر مورد ارزیاب باید اطمینان حاصل کند که قانون اول برای هر دو مورد با تولید بسته‌های کاربردپذیر و با استفاده از ابزار ضبط بسته و ثبت‌هایی برای تائید اعمال‌شده است. **آزمون ۲:** ارزیاب باید روش اجرایی بالا را تکرار کند به‌جز در این مورد که دو قانون باید به‌گونه‌ای در نظر گرفته شود که یکی زیرمجموعه‌ای از دیگری باشد (به‌عنوان مثال، یک نشانی خاص در مقابل بخشی از شبکه). ارزیاب باید مجدداً هر دو دستور را آزموده تا اطمینان حاصل کند که دستور اول بدون توجه به ویژگی قانون اجراشده است.

جدول ۲۱ اقدام تضمین الزام پالایش ترافیک VoIP۷

اقدام تضمین الزام کارکرد امنیتی پالایش ترافیک VoIP 7	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول فرایند اعمال قوانین پالایش ترافیک و همچنین رفتاری را (به‌طور پیش‌فرض و یا پیکربندی‌شده توسط مدیر سیستم) که برای انکار بسته‌ها هنگامی که از هیچ قانونی تبعیت نمی‌شود مگر آن‌که شرایط موردنیاز دیگری اجازه ترافیک شبکه بدهد را توصیف می‌کند (به‌عنوان مثال، FFW_ACL_EXT.1.5).

AGD	ارزیاب باید بررسی کند که مستندات راهنما هنگامی که هیچ قانون و یا شرایط خاصی برای ترافیک شبکه اعمال نمی‌شود، رفتار مناسب را توضیح دهد. اگر رفتار قابل پیکربندی باشد، ارزیاب باید بررسی کند که مستندات راهنما دستورالعمل‌های مناسب را برای پیکربندی رفتار برای انکار بسته‌هایی که منطبق بر قوانین نیستند را ارائه دهد.
Test	برای هر خصیصه در پالایش ترافیک VoIP وضعیت (حالت‌دار) (FFW_ACL_EXT.1.2)، ارزیاب باید آزمونی را ایجاد کند که نشان دهد محصول می‌تواند به‌درستی خصیصه‌های سربرگ بسته را با مجموعه قوانین مقایسه کرده و باید هم پذیرش و هم انکار را برای هر حالت نشان دهد. ارزیاب باید ثبت وقایع را در هر حالت بررسی کند تا تصدیق نماید که قوانین مرتبط اعمال‌شده است. ارزیاب باید یک ضبط بسته را برای هر آزمون ثبت کند تا رفتار درست محصول را نشان دهد.

جدول ۲۲ اقدام تضمین الزام پالایش ترافیک VoIP وضعیت (حالت‌دار) ۵

اقدام تضمین الزام کارکرد امنیتی پالایش ترافیک VoIP وضعیت (حالت‌دار) ۵	
TSS	ارزیاب باید بررسی نمایند که خلاصه مشخصه محصول توانایی محصول را برای انجام پالایش ترافیک وضعیت (حالت‌دار) تمامی پروتکل‌های VoIP مشخص‌شده در پالایش ترافیک VoIP وضعیت (حالت‌دار) (FFW_ACL_EXT.2.1) توضیح می‌دهد. همچنین ارزیاب باید بررسی کند که خلاصه مشخصه محصول قوانین پالایش ترافیک وضعیت (حالت‌دار) پیش‌فرضی را شناسایی می‌کند که توسط محصول به کار گرفته‌شده است و توضیح می‌دهد که هنگامی که ترافیک از یک یا چند مورد از این قوانین تخلف کند، چه اقداماتی اتخاذ می‌شوند. ارزیاب باید بررسی نمایند که خلاصه مشخصه محصول توانایی محصول در باز کردن و بستن پویای پورت‌ها را برای به کار بستن ترافیک VoIP توضیح می‌دهد به‌گونه‌ای که پورت‌های مورداستفاده برای انتقال ترافیک VoIP قابل پیش‌بینی نبوده و پورت‌ها جهت شنود ترافیک VoIP باز نیستند.
AGD	اگر محصول توانایی پیکربندی قوانین پالایش ترافیک وضعیت (حالت‌دار) را فراهم آورد، ارزیاب باید مستندات راهنما را مورد بازبینی قرار دهد تا بررسی نماید که این مستندات دستورالعمل‌هایی در مورد نحوه انجام این کار را ارائه می‌دهد.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** ارزیاب باید یک نقطه پایانی از راه دور را به محصول متصل کند و جایی که یک پیام BYE (پایان ارتباط) قبل از درخواست INVITE (دعوت) فرستاده‌شده است، از آن برای انتقال درخواست SIP خارج از توالی استفاده کند. ارزیاب باید با استفاده از ضبط‌های بسته و ثبت وقایع ممیزی بررسی کند که ترافیک خارج از توالی فرستاده‌شده است و تلاش برای تماس رهاشده و توسط محصول ثبت گردیده است. **آزمون ۲:**

	ارزیاب باید یک نقطه پایانی از راه دور را به محصول متصل کند و جایی که یک پاسخ RCF قبل از هر ترافیک دیگری فرستاده‌شده است، از آن برای انتقال درخواست H.225 خارج از توالی استفاده کند. ارزیاب باید با استفاده از ضبط‌های بسته و ثبت وقایع ممیزی بررسی کند که ترافیک خارج از توالی فرستاده‌شده است و تلاش برای تماس رهاشده و توسط محصول ثبت گردیده است. **آزمون ۳:** ارزیاب باید یک نقطه پایانی از راه دور را به محصول متصل کند و جایی که یک پیام پاسخ (ResponseMessage) قبل از یک پیام درخواست (RequestMessage) متناظر فرستاده‌شده است، از آن برای انتقال درخواست H.245 خارج از توالی استفاده کند. ارزیاب باید با استفاده از ضبط‌های بسته و ثبت وقایع ممیزی بررسی کند که ترافیک خارج از توالی فرستاده‌شده است و تلاش برای تماس رهاشده و توسط محصول ثبت گردیده است. **آزمون ۴:** اگر هدف امنیتی هر قانون پالایش ترافیک وضعیت (حالت‌دار) پیش‌فرض اضافه‌ای را مشخص کند، ارزیاب باید جریان ترافیک را به محصولی انتقال دهد که هر یک از این قوانین را نقض می‌کند و با استفاده از ضبط‌های بسته و ثبت وقایع ممیزی مشاهده کند که در تمامی حالت‌های تماس، محصول ترافیک نامعتبر را رها کرده و آن را ثبت می‌کند. **آزمون ۵:** یک فهرست کنترل دسترسی (ACL) سفارشی را جهت رد تماس آغازشده از یک زیرشبکه یا نشانی IP پیکربندی کرده، تماسی از آن نشانی IP یا زیرشبکه برقرار کرده و بررسی شود که تماس کامل انجام نمی‌شود. بررسی شود که تماس‌ها از دیگر نشانی‌های IP یا هر زیر شبکه دیگری یک تماس کامل خواهد بود. **آزمون ۶:** تماسی را انجام داده و بسته‌ها را ضبط کنید. ضبط‌های بسته بررسی‌شده و از پورت‌های کانال رسانه‌ای (RTP، SRTP) که ارتباط بر روی آن انجام‌شده است یادداشت‌برداری شود. تماس را خاتمه داده، با استفاده از یک تولیدکننده بسته، اقدام به ارسال ترافیک بر روی پورت‌های رسانه‌ای شود که هنگامی که تماس فعال بود فعال بودند. با استفاده از ضبط‌های بسته، بررسی شود که ترافیک بر روی این پورت‌ها از محصول عبور نمی‌کند.

جدول ۲۳ اقدام تضمین الزام بازرسی عمیق بسته ۳

اقدام تضمین الزام کارکرد امنیتی بازرسی عمیق بسته ۳	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول را برای اجرای بازرسی عمیق بسته برای H.323، SIP، RTP و ترافیک RTCP و قوانینی که محصول جهت تعیین اینکه آیا ترافیک دریافت شده به‌خوبی شکل‌گرفته است را توضیح دهد. همچنین ارزیاب باید بررسی کند که خلاصه مشخصه محصول توضیح دهد هنگامی که یک ترافیک ناقص شناسایی‌شده باشد، محصول چه اقداماتی را انجام می‌دهد.
AGD	اگر تابع بازرسی عمیق بسته محصول قابل تنظیم باشد، ارزیاب باید بررسی کند که مستندات راهنما دستورالعمل‌هایی در مورد نحوه پیکربندی این تابع فراهم آورده است.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** اگر تابع بسته عمیق قابل تنظیم باشد، ارزیاب باید توجه به انتخاب انجام‌شده در بازرسی عمیق بسته (FFW_DPI_EXT.1.3)، این تابع را برای پرچم‌دار کردن، ثبت و یا رها کردن ترافیک ناقص H.225 پیکربندی کند. سپس ارزیاب باید ترافیک ناقص H.225 را به محصول انتقال دهد. با استفاده از ضبط‌های بسته و ثبت ممیزی، ارزیاب باید بررسی کند که ترافیک ناقص به محصول فرستاده‌شده، ثبت گردیده و هیچ‌چیز بیشتری را انتقال ندهد. ارزیاب باید برای هر یک از انواع ترافیک ناقص H.225 که طبق توضیحات موجود در بازرسی عمیق بسته (FFW_DIP_EXT.1.2) می‌تواند توسط محصول تشخیص داده شود این آزمون را تکرار کند. **آزمون ۲:** ارزیاب باید آزمون ۱ را برای ترافیک H.245 تکرار کند. **آزمون ۳:** ارزیاب باید آزمون ۱ را برای ترافیک SIP تکرار کند. **آزمون ۴:** ارزیاب باید آزمون ۱ را برای ترافیک RTP تکرار کند. **آزمون ۵:**

	ارزیاب باید آزمون ۱ را برای ترافیک RTCP تکرار کند.

جدول ۲۴ اقدام تضمین الزام پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه (NAT)

اقدام تضمین الزام کارکرد امنیتی پنهان کردن همبندی یا پیمایش برگردان نشانی شبکه 4 (NAT)	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول را جهت پشتیبانی از برگردان نشانی شبکه (NAT) برای پروتکل‌های مشخص‌شده در پنهان کردن همبندی (ریخت‌شناسی) یا پیمایش برگردان نشانی شبکه (FFW_NAT_EXT.1.2) (NAT) توضیح داده است. علاوه بر آن ارزیاب باید بررسی کند که خلاصه مشخصه محصول توضیح دهد که چگونه محصول از برگردان نشانی شبکه (NAT) برای جایگزینی مقادیر سربرگ نشانی IP ترافیک خارج از محدوده استفاده می‌کند و چگونه رد هویت اصلی طرف‌های تماس‌گیرنده را نگهداری می‌کند.
AGD	اگر نویسنده هدف امنیتی «یک مقدار تعریف‌شده مدیر سیستم امنیتی» را در پنهان کردن همبندی (ریخت‌شناسی) یا پیمایش برگردان نشانی شبکه (NAT) (FFW_NAT_EXT.1.3)) انتخاب کند، ارزیاب باید مستندات راهنما را بررسی کند تا دستورالعمل‌هایی برای نحوه تعریف مقدار سربرگ نشانی IP فراهم‌شده باشد.
Test	ارزیاب باید یک تماس آغازشده از «شبکه داخلی» به «شبکه خارجی» برقرار کند. ارزیاب باید از ضبط‌های بسته بر روی شبکه «خارجی» استفاده کند تا بررسی کند که داده‌های بسته ساختار آدرس‌دهی یا نام‌گذاری شبکه «داخلی» را فاش نمی‌کند. اگر نویسنده هدف امنیتی «یک مقدار تعریف‌شده مدیر سیستم امنیتی» را در پنهان کردن همبندی (ریخت‌شناسی) یا پیمایش برگردان نشانی شبکه (NAT) (FFW_NAT_EXT.1.3)) انتخاب کند، ارزیاب باید یک مقدار سربرگ IP داده‌شده را مشخص کرده و تائید کند که ترافیک مقدار سربرگ اصلی را با مقدار تعریف‌شده مدیر سیستم جایگزین می‌کند. اگر نویسنده هدف امنیتی، به‌جای آن «نشانی IP محصول» را انتخاب کرد، ارزیاب باید بررسی کند که این مقدار سربرگ نشانی IP رابط شبکه «خارجی» محصول است.

جدول ۲۵ اقدام تضمین الزام کارکرد امنیتی سرور پروتکل آغاز نشست (SIP)

اقدام تضمین الزام کارکرد امنیتی سرور پروتکل آغاز نشست (SIP) 4	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول را برای پشتیبانی از SIP مطابق با RFC 3261 توضیح دهد، این توانایی شامل الزام احراز هویت کلمه عبور برای درخواست‌های تابع ثبت‌نام (SIP REGISTER) است. ارزیاب باید بررسی کند که خلاصه مشخصه محصول ترکیب‌های مجاز کلمه‌های عبور احراز هویت SIP را نیز توضیح می‌دهد. ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول را برای تغییر مقادیر سربرگ ترافیک SIP قبل از انتقال مجدد ترافیک برای ترافیک SIP دریافت شده توسط محصول فراهم می‌آورد.
AGD	ارزیاب باید بررسی کند که مستندات راهنما نشان دهند که درخواست‌های ثبت‌نام SIP باید همراه با حداقل استحکام کلمه عبور موردنیاز برای اعتبارنامه احراز هویت توسط محصول احراز اصالت شوند. همچنین ارزیاب باید بررسی کند که مستندات راهنما دستورالعمل‌هایی برای نحوه پیکربندی محصول برای اجرای مقادیر سربرگ SIP را فراهم آورد.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** برای داشتن یک سرویس‌گیرنده (کلاینت) SIP برای صدور یک درخواست ثبت‌نام (REGISTER) بدون ارائه اعتبارنامه‌های احراز هویت اقدام شود. مشاهده شود که درخواست توسط محصول رد شده و ثبت گردیده است. **آزمون ۲:** برای داشتن یک سرویس‌گیرنده (کلاینت) SIP برای صدور یک درخواست ثبت‌نام (REGISTER) با اعتبارنامه‌های احراز هویت و با استفاده از نویسه‌های پشتیبانی نشده توسط محصول اقدام شود. مشاهده شود که درخواست توسط محصول رد شده و ثبت گردیده است. **آزمون ۳:** برای داشتن یک سرویس‌گیرنده (کلاینت) SIP برای صدور یک درخواست ثبت‌نام (REGISTER) با اعتبارنامه‌های احراز هویت معتبر با استفاده از نویسه‌های پشتیبانی شده توسط محصول اقدام شود. مشاهده شود که درخواست توسط محصول پذیرفته‌شده و ثبت گردیده است. این آزمون باید به‌دفعات زیادی تکرار شود تا

	اطمینان حاصل شود که کلمه‌های عبور با حداقل و حداکثر طول‌های پشتیبانی شده مورداستفاده قرارگرفته است و هر نویسه پشتیبانی شده حداقل در یک کلمه عبور مورداستفاده قرارگرفته است. **آزمون ۴:** محصول برای اجرای مقادیر سربرگ SIP پیکربندی کنید. تماسی را از طریق محصول برقرار کرده، ترافیک را قبل از اینکه توسط محصول دریافت شود و بعد از اینکه از محصول خارج شد ضبط کرده، بررسی شود که مقادیر سربرگ SIP تغییریافته باشد. در صورت لزوم آزمون را برای هر تغییر سربرگ پشتیبانی شده تکرار کنید.

جدول ۲۶ اقدام تضمین الزام کانال دهی پروتکل آغاز نشست (SIP)

اقدام تضمین الزام کارکرد امنیتی کانال دهی پروتکل آغاز نشست 4 (SIP)	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول در پشتیبانی از کانال دهی SIP احراز هویت شده و رمزگذاری شده را به همراه روش‌هایی که کانال‌های نظیر را برای محصول احراز هویت خواهند کرد، توضیح داده است.
AGD	ارزیاب باید مستندات راهنما را بررسی کند تا درصورتی‌که رمزگذاری و احراز هویت قابل پیکربندی باشد، دستورالعمل‌هایی برای نحوه پیکربندی کانال دهی SIP که مستلزم رمزگذاری و احراز هویت است ارائه دهد.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** محصول برای پشتیبانی از یک کانال SIP رمزگذاری شده پیکربندی‌شده، کانال نظیری برای ارتباط با محصول با استفاده از کانال SIP پیکربندی شود. ترکیب درستی از نام کاربری و کلمه عبور بر روی کانال نظیر همراه با یک درخواست کانال SIP ارائه شود که از یک نشانی IP خارجی منشأ می‌گیرد. با ضبط‌های بسته و ثبت‌های ممیزی بررسی شود که نشست برقرارشده است. **آزمون ۲:** آزمون ۱ با ارائه اطلاعات نام کاربری و کلمه عبور اشتباه با کانال نظیر تکرار شود و با ضبط‌های بسته و ثبت‌های ممیزی بررسی شود که نشست برقرار نشده است.

	آزمون ۳: آزمون ۱ با تغییر در نشانی IP کانال نظیر تکرار شود و با ضبط‌های بسته و ثبت‌های ممیزی بررسی شود که نشست برقرار نشده است.

جدول ۲۷ اقدم تضمین الزام اولویت‌بندی محدود خدمت ۲

اقدام تضمین الزام کارکرد امنیتی اولویت‌بندی محدود خدمت ۲	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول توانایی محصول برای اولویت‌بندی جریان ترافیک و همچنین سازوکاری که با آن دسترسی به پهنای باند شبکه توسط محصول اعطا می‌گردد را توصیف کرده باشد.
AGD	ارزیاب باید مستندات راهنما را موردبررسی قرار دهد تا شامل تشریحی برای نحوه پیکربندی کیفیت خدمت[۱] (QoS) برای محصول باشد، از جمله نحوه تنظیم برچسب‌ها برای جریان‌های ترافیک داده‌شده.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** محصول را جهت پشتیبانی از کیفیت خدمت (QoS) پیکربندی کرده. برچسب‌های کیفیت خدمت (QoS) را برای جریان‌های رسانه و ترافیک سیگنال دهی تنظیم کرده. تماسی بین طرف‌های تماس‌گیرنده که از طریق دو رابط مختلف خارجی به محصول متصل شده‌اند برقرارشده. با استفاده از ضبط بسته بررسی شود که ترافیک بین محصول و دریافت‌کننده تماس با علائم کیفیت خدمت (QoS) مناسب برچسب‌گذاری شده است. **آزمون ۲:** محصول را جهت پشتیبانی از کیفیت خدمت (QoS) پیکربندی کرده. برچسب‌های کیفیت خدمت (QoS) را برای جریان‌های رسانه و ترافیک سیگنال دهی تنظیم کرده. یک نقطه پایانی از راه دور را پیکربندی کرده تا به‌عنوان طرف تماس‌گیرنده‌ای عمل کند که جریان پیوسته‌ای از ترافیک VoIP (سیگنال دهی و رسانه) را به نقطه پایانی دیگری ارسال می‌کند که از طریق یک رابط خارجی متفاوت به محصول متصل شده است. با استفاده از ضبط بسته بررسی شود که ترافیک بین محصول و

[۱] Quality of Service

	دریافت‌کننده تماس با علائم کیفیت خدمت (QoS) مناسب برچسب‌گذاری شده است و فاکتور R کیفیت خدمت (QoS) تا زمانی که ترافیک ادامه می‌یابد به‌روزرسانی می‌شود.

جدول ۲۸ اقدام تضمین الزام حداکثر سهمیه‌ها ۱

اقدام تضمین الزام کارکرد امنیتی حداکثر سهمیه‌ها ۱	
TSS	ارزیاب باید بررسی کند که خلاصه مشخصه محصول منابع داخلی را که با استفاده از آن محصول می‌توانند از حملات انکار خدمت (DoS) جلوگیری کرده توضیح داده و همچنین انواع رفتارهایی که یک حمله انکار خدمت (DoS) را در مقابل هر یک از این منابع تشکیل می‌دهد را توصیف کند.
AGD	اگر توانایی محافظت در برابر حمله انکار خدمت (DoS) قابل پیکربندی باشد. ارزیاب باید بررسی کند که راهنماهای عملیاتی دستورالعمل‌هایی در مورد نحوه پیکربندی این تابع را فراهم آورد.
Test	ارزیاب باید آزمون‌های زیر را انجام دهد: **آزمون ۱:** با استفاده از ابزار انتخاب، اقدام به یک حمله انکار خدمت (DoS) شده که چرخه‌های اضافی CPU را ایجاد می‌کند. هنگامی که این حمله اتفاق می‌افتد تماسی برقرار شود. از طریق ضبط بسته و فایل صوتی یا تصاویر صفحه‌نمایش[۱] بررسی شود که تماس موفقیت‌آمیز بوده است. **آزمون ۲:** با استفاده از ابزار انتخاب، اقدام به یک حمله انکار خدمت (DoS) شده که موجب استفاده از کل حافظه[۲] می‌شود. هنگامی که این حمله اتفاق می‌افتد تماسی برقرار شود. از طریق ضبط بسته و فایل صوتی یا تصاویر صفحه‌نمایش بررسی شود که تماس موفقیت‌آمیز بوده است. **آزمون ۳:**

[۱] screenshot

[۲] exhaust

	با اســتفاده از ابزار انتخاب، اقدام به حمله انکار خدمت توزیع‌شــده (DDoS) در برابر رابط (های) شــبکه خارجی محصــول شــود. هنگامی که این حمله اتفاق می‌افتد تماسی برقرار شود. از طریق ضبط بسته و فایل صوتی یا تصاویر صفحه‌نمایش بررسی شود که تماس موفقیت‌آمیز بوده است. **آزمون ۴:** با اســتفاده از ابزار انتخاب، فازی کردن پروتکل را برای هر پروتکل ارتباطی پشــتیبانی شــده توسط محصول انجام داده، بررسی شود که فازی کردن پروتکل موجب به خطر افتادن محصول و یا تجربه قابلیت‌های کارکردی تضعیف‌شده نمی‌شود. برای هر ابزار انتخاب مورداستفاده برای انجام این آزمون‌ها، ارزیاب باید استدلالی برای مناسب بودن ابزار انتخاب‌شده ارائه دهد.

جدول ۲۹ اقدام تضمین الزام کانال امن درون محصول ۳ (۲)

اقدام تضمین الزام کارکرد امنیتی کانال امن درون محصول ۳ (۲)
این الزام کارکرد امنیتی تکرار کانال امن درونی محصــول (FTP_ITC.1) تعریف‌شــده در پروفایل حفاظتی مشــترک افزاره شــبکه (NDcPP) اســت. ارزیاب باید فعالیت‌های تضــمین تعریف‌شده برای کانال امن درونی محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را برای تکرار این الزام کارکرد امنیتی تکرار کند.

جدول ۳۰ اقدام تضمین الزام کانال امن درون محصول ۳ (۳)

اقدام تضمین الزام کارکرد امنیتی کانال امن درون محصول ۳ (۳)
این الزام کارکرد امنیتی تکرار کانال امن درونی محصــول (FTP_ITC.1) تعریف‌شــده در پروفایل حفاظتی مشــترک افزاره شــبکه (NDcPP) اســت. ارزیاب باید فعالیت‌های تضــمین تعریف‌شده برای کانال امن درونی محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را برای تکرار این الزام کارکرد امنیتی تکرار کند.

جدول ۳۱ اقدام تضمین الزام کانال امن درون محصول ۳ (۴)

اقدام تضمین الزام کارکرد امنیتی کانال امن درون محصول ۳ (۴)

این الزام کارکرد امنیتی تکرار کانال امن درونی محصول (FTP_ITC.1) تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) است. ارزیاب باید اقدامات تضمین تعریف‌شده برای کانال امن درونی محصول (FTP_ITC.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را برای تکرار این الزام کارکرد امنیتی تکرار کند.

۷- منطق الزامات امنیتی

تمرکز بخش‌های اولیه سند بسته الحاقی، روایتی به‌منظور افزایش فهم کلی تهدیدات موردتوجه کنترل‌کننده‌های محدوده نشست، روش‌های مورداستفاده برای کاهش این تهدیدات و میزان کاهش به‌دست‌آمده با محصول منطبق بر این بسته الحاقی است. به دلیل آن‌که این سبک روایت گونه به‌آسانی به یک فعالیت ارزیابی رسمی قابل اضافه کردن نیست، بنابراین این پیوست شامل ابزارهای جدولی است که می‌تواند برای اقدامات ارزیابی مربوط به این سند استفاده شود.

۷-۱- تعریف مسئله امنیتی

۷-۱-۱- مفروضات

هیچ فرضی برای این بسته الحاقی تعریف‌نشده است. به‌عنوان یک بسته الحاقی برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)، محصول تمامی مفروضات تعریف‌شده توسط پروفایل حفاظتی مبنا به‌جز مفروضات تعریف‌شده در قسمت ۳-۲- این بسته الحاقی را به ارث می‌برد.

۷-۱-۲- تهدیدات

جدول زیر فهرستی از تهدیداتی که توسط کنترل‌کنندگان محدود نشست منطبق بر این بسته الحاقی تضعیف‌شده است را نشان می‌دهد. توجه داشته باشید که تمام تهدیدات تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) توسط این بسته الحاقی به ارث برده می‌شوند. چنانچه تهدیدی از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) در اینجا مجدداً تولیدشده باشد، بدان معناست که این بسته الحاقی الزامات کارکرد امنیت اضافه‌ای را برای تضعیف تهدید به روشی خاص‌تر نسبت به آنچه در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تعیین‌شده است تعریف می‌کند.

جدول ۳۲ تهدیدات

نام تهدید	تعریف تهدید
T.NETWORK_DISCLOSURE	ممکن است یک مهاجم اقدام به ترسیم زیرشبکه‌ای برای تعیین افزاره‌های مستقر بر روی شبکه و به دست آوردن نشانی‌های IP ماشین‌ها و خدماتی (پورت‌هایی) که آن ماشین‌ها ارائه می‌دهند نماید. این اطلاعات می‌تواند برای شروع حملات به آن ماشین‌ها از طریق خدمات در معرض خطر استفاده شود.
T.MALICIOUS_TRAFFIC	ممکن است مهاجم اقدام به ارسال بسته‌های ناقص به کنترل‌کننده محدوده نشست (SBC) کند، به امید آن‌که موجب شنود پشته شبکه یا خدمات از پورت‌های UDP/TCP بر روی کنترل‌کننده محدوده نشست (SBC) و یا درهم شکستن شبکه حفاظت‌شده شود.
T.UNTRUSTED_COMMUNICATION_CHANNELS	به دلیل وجود کانال ارتباطی غیر امن که باعث افشای داده در حین انتقال می‌شود ممکن است، مهاجم داده کاربر یا داده حساس محصول را به دست آورد که به محصول و یا از آن انتقال‌یافته است.
T.NETWORK_ACCESS	ممکن است مهاجم ترافیکی را از طریق محصول بفرستد که آن‌ها را قادر به دسترسی بدون ارائه احراز هویت به افزاره‌های محیط عملیاتی محصول می‌کند.
T.USER_DATA_REUSE	ممکن است داده کاربر به‌صورت غیرعمدی به مقصدی فرستاده شود که مدنظر فرستنده اصلی نبوده و باعث افشای غیرمجاز داده می‌شود.
T.RESOURCE_EXHAUSTION	ممکن است یک مهاجم ترافیک شبکه را به محصول انتقال دهد که باعث می‌شود محصول قادر به انجام وظایف خود بر روی ترافیک شبکه مشروع نباشد.

۷-۱-۳-خط‌مشی‌های امنیتی سازمانی

هیچ خط‌مشی سازمانی مختص کنترل‌کننده محدوده نشست (SBC) شناسایی نشده است. هرچند تمام خط‌مشی‌های امنیتی سازمان در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) برای کنترل‌کننده محدوده نشست (SBC) به کار گرفته می‌شود.

۷-۱-۴- تناظر تعریف مسئله امنیتی

جدول زیر نگاشتی از تهدیدات و مفروضات تعریف‌شده در این بسته الحاقی را برای اهداف امنیتی تعریف‌شده و مشخص‌شده در این بسته الحاقی ارائه می‌دهد.

جدول ۳۳ تناظر تعریف مسئله امنیتی

تهدید یا فرض	اهداف امنیتی
T.NETWORK_DISCLOSURE	O.TOPOLOGY_HIDING, O.USER_DATA_DELIVERY
T.MALICIOUS_TRAFFIC	O.TRAFFIC_FILTERING
T.UNTRUSTED_COMMUNICATION_CHANNELS	O.PROTECTED_COMMUNICATIONS
T.NETWORK_ACCESS	O.TRAFFIC_FILTERING, O.USER_DATA_DELIVERY
T.USER_DATA_REUSE	O.USER_DATA_DELIVERY
T.RESOURCE_EXHAUSTION	O.RESOURCE_AVAILABILITY

به یاد داشته باشد که این بسته الحاقی شامل اهداف امنیتی است که تهدیداتی را از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا به شیوه‌ای دقیق‌تر، بر اساس توابع خاص ارائه‌شده توسط کنترل‌کننده محدوده نشست (SBC) محصول موردتوجه قرار می‌دهد:

- هدف امنیتی سامانه ناظر (O.SYSTEM_MONTORING) تهدید اقدام شناسایی نشده (T.UNDETECTED_ACTIVITY) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را بیشتر تضعیف می‌کند.
- هدف مدیریتی مجاز (O.AUTHORIZED_ADMINISTRATION) تهدید مدیر سیستم غیرمجاز (T.UNAUTHORIZED_ADMINISTRATOR_ACCESS) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را بیشتر تضعیف می‌کند.

۷-۲- اهداف امنیتی

۷-۲-۱-اهداف امنیتی محصول

جدول زیر شامل اهداف امنیتی خاص کنترل‌کننده محدوده نشست است.

جدول ۳۴- اهداف امنیتی برای محصول

نام هدف	تعریف هدف
O.SYSTEM_MONITORING	محصـــول ابزاری فراهم می‌آورد کـه هنگـامی کـه رویداد مرتبط با امنیتی رخ می‌دهد را تشـــخیص داده و رویدادهای ممیزی و یا هشدارهای امنیتی را در پاسخ به این تشخیص تولید می‌کند.
O.PROTECTED_COMMUNICATIONS	محصول ابزاری برای ایجاد کانال‌های ارتباطی امن بین محصول و محیط عملیاتی فراهم می‌آورد.
O.TOPOLOGY_HIDING	محصول توانایی جلوگیری از افشای اطلاعات مرتبط با افزاره‌هایی که در شبکه محافظت‌شده خود قرارگرفته‌اند را فراهم می‌آورد.
O.TRAFFIC_FILTERING	محصول توانایی برای اجرای قوانین پالایش ترافیک شبکه و رها کردن ترافیکی که غیرمجاز و یا ناقص است را فراهم می‌آورد.
O.USER_DATA_DELIVERY	محصـــول ســـازوکارهایی برای حصـــول اطمینان از اینکه داده کاربر انتقال‌یافته بین طرف‌های تماس‌گیرنده تنها به گیرنده(های) موردنظر معطوف شده است فراهم می‌آورد.
O.RESOURCE_AVAILABILITY	محصـول سازوکارهایی برای اولویت‌بندی ترافیک شبکه و محافظت در برابر حملات انکار خدمت فراهم آورده تا اطمینان حاصل کند که پهنای باند آن به‌طور اثربخشی مورداستفاده قرارگرفته است.
O.AUTHORIZED_ADMINISTRATION	محصول توابع مدیریتی فراهم می‌آورد که می‌تواند برای مدیریت امن محصول مورداستفاده قرار گیرد.

۷-۲-۲- اهداف امنیتی محیط عملیاتی

در این بسته الحاقی هیچ‌گونه اهداف امنیتی محیطی تعریف‌نشده است. به‌عنوان یک بسته الحاقی برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)، محصول تمامی اهداف امنیتی محیطی تعریف‌شده توسط پروفایل حفاظتی مبنا را به‌جز موردی که در بخش ۴-۲ این بسته الحاقی تعریف‌شده است به ارث می‌برد.

۷-۲-۳- تناظر اهداف امنیتی

تناظر بین الزامات کارکرد امنیتی (SFR) و اهداف امنیتی شناسایی‌شده و یا تعریف‌شده در این بسته الحاقی در بخش ۴ ارائه‌شده است.

پیوست ۱ الزامات اختیاری

الزامات پایه در متن این بسته الحاقی گنجانده‌شده است. الزامات اضافی می‌توانند در هدف امنیتی گنجانده شوند، اما برای محصولی که ادعای انطباق با این بسته الحاقی را دارد اجباری نیست. لزومی ندارد که تمام کنترل‌کننده‌های محدوده نشست به‌عنوان سامانه‌های توزیع یافته اجرا شوند؛ بنابراین، الزامات این پیوست در متن این بسته الحاقی گنجانده نشده‌اند. در حالتی که محصول به‌صورت فیزیکی بین مؤلفه‌های مختلف توزیع‌شده است، ارتباطات بین آن مؤلفه‌ها باید محافظت‌شده و الزامات زیر باید در هدف امنیتی گنجانده شود.

نکته: نویسنده هدف امنیتی مسئول حصول اطمینان از این موضوع است که الزاماتی که ممکن است با الزامات موجود در پیوست ۱، پیوست ۲ و یا پیوست ۳ مرتبط باشند اما ذکر نشده‌اند (به‌عنوان مثال الزامات از نوع FMT) در هدف امنیتی نیز گنجانده‌شده باشند.

این نسخه از بسته الحاقی هیچ الزام اختیاری را تعریف نکرده است.

پیوست ۲ الزامات مبتنی بر انتخاب

الزامات پایه (الزاماتی که باید توسط محصول و یا بستره زیرین اعمال شود) در متن این بسته الحاقی گنجانده‌شده است. الزامات اضافی مبتنی بر انتخاب در متن بسته الحاقی گنجانده‌شده‌اند: چنانچه انتخاب معینی انجام شود، لازم است الزامات اضافی زیر گنجانده شود.

در حال حاضر هیچ الزام مبتنی بر انتخابی توسط این بسته الحاقی تعیین نشده است.

پیوست ۳ الزامات هدف

الزامات پایه (الزاماتی که باید توسط محصول و یا بسته زیرین آن اعمال شود) در متن این بسته الحاقی گنجانده‌شده است. الزامات اضافی که قابلیت‌های کارکردی امنیتی مطلوب را مشخص می‌کند در این پیوست گنجانده‌شده است. انتظار می‌رود که این الزامات در نسخه‌های آینده این بسته الحاقی از الزامات هدف به الزامات پایه انتقال یابد.

در حال حاضر، هیچ الزامات هدفی خاص کنترل‌کننده محدوده نشست (SBC) محصول شناسایی نشده است.

پیوست ۴ نمادها و اختصارات

نماد	معادل انگلیسی	معادل فارسی
ACL	Access Control List	فهرست کنترل دسترسی
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
B2BUA	Back-to-back user agent	عامل کاربر پشت‌به‌پشت
CDR	Call Detail Record	ثبت جزئیات تماس
DPI	Deep packet inspection	بازرسی بسته عمیق
DoS	Denial of Service	انکار خدمت
EP	Extended Package	بسته الحاقی
IP PBX	Private Branch Exchange with Internet Protocol	تبادل انشعاب خصوصی با پروتکل اینترنتی
IPsec	Internet Protocol Security	امنیت پروتکل اینترنت
NAT	Network address translation	برگردان نشانی شبکه
NDcPP	Network Device Collaborative Protection Profile	پروفایل حفاظتی مشترک افزاره شبکه
NTP	Network Time Protocol	پروتکل زمانی شبکه
PP	Protection Profile	پروفایل حفاظتی
QoS	Quality of Service	کیفیت خدمت
SCB	Session Border Controller	کنترل‌کننده محدوده نشست
SDES	Media Streams	جریان‌های رسانه‌ای

SDP	Session Description Protocol	پروتکل توصیف نشست
SFR	Security functional requirements	الزامات کارکرد امنیتی
SIP	Session initiation protocol	پروتکل آغاز نشست
SRTP	Secure Real-time Transport Protocol	پروتکل انتقال بلادرنگ امن
ST	Security Objective	هدف امنیتی
TLS	Transport Layer Security	امنیت لایه انتقال
TOE	Target of Evaluation	محصول
TSS	TOE Summary Specification/TSS	خلاصه مشخصه محصول
VoIP	Voice over Internet Protocol	صدا بر روی پروتکل اینترنتی
SFP	Security Functionality Policy	خط‌مشی کارکرد امنیتی