به نام خدا

بسته الحاقی پروفایل حفاظتی مشترک افزاره شبکه/پروفایل حفاظتی نرم‌افزار کاربردی برای سرورهای احراز هویت

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

این بسته الحاقی (EP)[۱] الزامات امنیتی را برای سرور احراز هویت تشریح می‌کند و برای ارائه مجموعه حداقلی از الزامات برای کاهش تهدیدات معین و تعریف‌شده در نظر گرفته شده است. محصولات سرور احراز هویت به سازمان‌ها اجازه می‌دهند تا روشی استاندارد و متمرکز برای ارزیابی درخواست‌های احراز هویت کاربران در سراسر سازمان ایجاد کنند. این کار تعریف متمرکز هویت کاربر و داده اعتبارنامه[۲] را امکان‌پذیر می‌کند و امکان به‌کارگیری یکسان خط‌مشی‌های احراز هویت را فراهم می‌آورد که اعتبارنامه‌ها و خصیصه‌های کاربری لازم برای کسب دسترسی به برنامه‌های کاربردی و سامانه‌های متفاوت در محیط سازمان را تعریف می‌کند. این بسته الحاقی به‌صورت خاص بر روی خدمت احراز هویت از راه دور کاربران تماس‌گیرنده (RADIUS)[۳] سرورهای احراز هویت تمرکز دارد.

این بسته الحاقی، پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)[۴] را برای شرایط نصب سرور احراز هویت بر روی تجهیزات شبکه اختصاصی تأمین‌شده از جانب فروشنده محصول گسترش می‌دهد. همچنین این بسته الحاقی پروفایل حفاظتی برنامه کاربردی (App PP)[۵] را برای شرایطی که سرور احراز هویت یک برنامه کاربردی نرم‌افزاری بوده و بر روی یک کامپیوتر عمومی نصب شده باشد و این کامپیوتر توسط فروشنده محصول تأمین نشده است، گسترش می‌دهد.

---

[۱] Extended Package (EP)

[۲] credential

[۳] Remote Authentication Dial In User Service (RADIUS)

[۴] Network Device Collaborative Protection Profile

آنچه در زمینه به‌کارگیری بسته الحاقی به همراه پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) یا پروفایل حفاظتی برنامه کاربردی (App PP) انتظار می‌رود این است که محتوای این بسته الحاقی و پروفایل حفاظتی انتخاب‌شده، به‌طور مناسب در زمینه هر هدف امنیتی خاص محصول[۶] ترکیب شوند. این بسته الحاقی به‌صورت خاص به‌گونه‌ای تعریف شده است تا در به‌کارگیری آن هیچ‌گونه ابهام و مشکلی وجود نداشته باشد. زمانی که این بسته الحاقی همراه با پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) یا پروفایل حفاظتی برنامه کاربردی (App PP) استفاده می‌شود محصول منطبق با آن، ملزم به پیاده‌سازی الزامات کارکردی مورد نیاز در آن پروفایل‌های حفاظتی به همراه کارکردهای اضافی تعریف‌شده در این بسته الحاقی است تا در مقابل محیط تهدید که در ادامه مورد بحث قرار می‌گیرد پاسخگو باشد. هدف امنیتی باید نسخه‌های کاربردپذیر پروفایل حفاظتی منتخب و این بسته الحاقی را در قبال ادعای انطباق خود شناسایی کند.

---

[۵] Application Software Protection Profile

[۶] Product-specific

۲- شرح محصول

این سند الزامات کارکرد امنیتی سرور احراز هویت را بیان می‌کند. یک سرور احراز هویت به‌منظور احراز هویت موجودیتی (کاربر یا افزاره شبکه) که قصد دسترسی به شبکه محافظت‌شده را دارد، طراحی شده است. سرور دسترسی شبکه (NAS)[۷] اعتبارنامه‌های احراز هویت[۸] (مدارک احراز هویت) را به سرور احراز هویت ارسال می‌کند؛ سرور احراز هویت اعتبارنامه‌ها را بررسی کرده و مجاز بودن کاربر یا افزاره شبکه را تعیین می‌کند. سرور احراز هویت تعریف شده توسط این بسته الحاقی می‌تواند یک افزاره اختصاصی مستقل یا یک برنامه کاربردی باشد که بر روی سامانه دیگری در محیط عملیاتی اجرا می‌شود. سرور احراز هویت می‌تواند با سرور دسترسی شبکه در یک مکان نصب‌شده یا جدا از آن باشد.

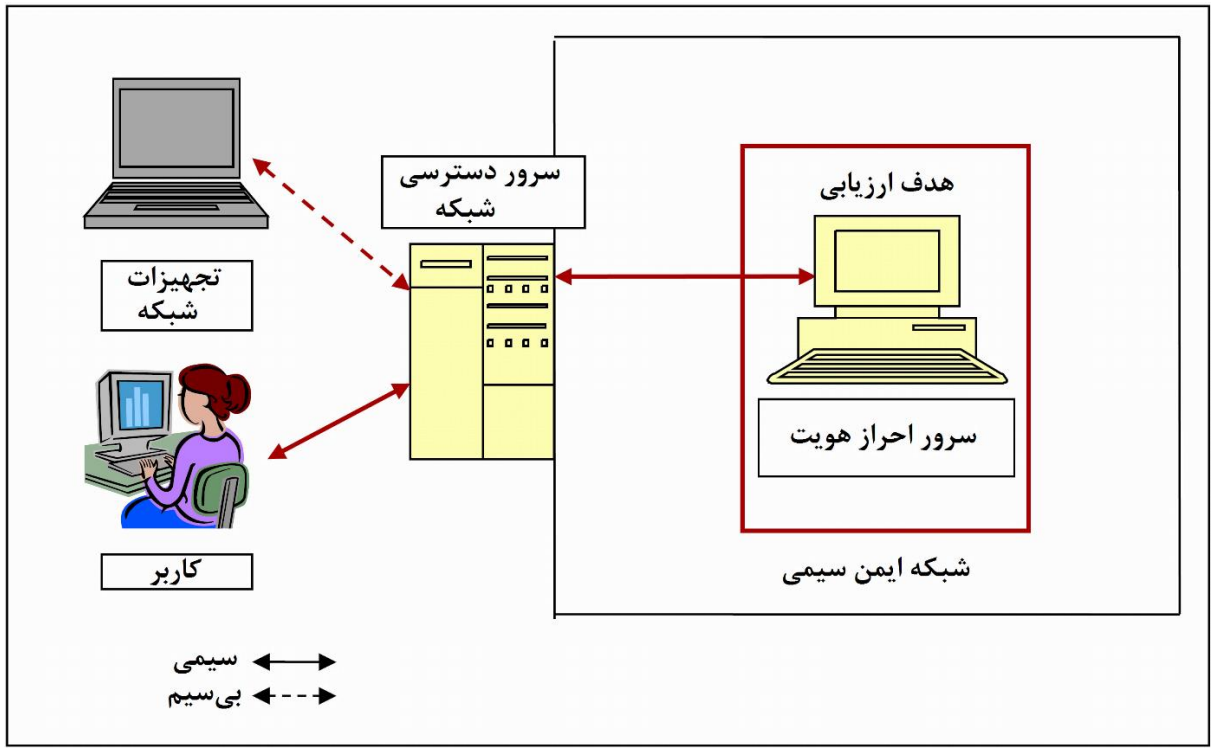
سرور احراز هویت می‌تواند بخشی از یک سرور احراز هویت، اعطای مجوز و حسابرسی[۹] (AAA Server) باشد. احراز هویت، موجودیت را شناسایی می‌کند، اعطای مجوز، خط‌مشی‌های کنترل دسترسی را به اجرا می‌گذارد و حسابرسی، پیگیری منابع برای تحلیل و صدور صورتحساب را دربر دارد. این بسته الحاقی الزامات کارکردی را فقط برای خدمات احراز هویت سرورهای احراز هویت، اعطای مجوز و حسابرسی (AAA Server) مشخص می‌کند. در شکل ۱، شبکه‌ای با سرور احراز هویت نشان شده است.

---

[۷] Network Access Server (NAS)

[۸] Authentication Credentials

[۹] Authentication, Authorization and Accounting Server



شکل ۱ شبکه با سرور احراز هویت

۲-۱- کاربری و ویژگی‌های اصلی امنیتی محصول

سرورهای احراز هویت در پشتیبانی از یک سرور دسترسی شبکه (NAS) برای احراز هویت افزاره و یا کاربر بکار می‌روند. برای مثال، ممکن است سامانه شبکه محلی بی‌سیم (WLAN)[۱۰] از خدمات سرور اختصاصی احراز هویت در مدت زمان برقراری تونل استفاده کند، در نتیجه سرور احراز هویت باید از کنترل دسترسی شبکه مبتنی بر پورت[۱۱] IEEE 802.1X پشتیبانی کند و نقش سرور احراز هویت IEEE 802.11 را بر عهده بگیرد. چارچوب معماری کنترل دسترسی مبتنی بر پورت، سه نقش جداگانه تعریف می‌کند: درخواست‌کننده (سرویس گیرنده)، احراز هویت کننده[۱۲] (NAS) و سرور احراز هویت (محصول). بسته به سرور احراز هویت ممکن است سرور دسترسی شبکه (NAS) از درخواست‌کننده بخواهد تا احراز هویت 802.1X را قبل از ارائه دسترسی به شبکه انجام دهد. سرور دسترسی شبکه (NAS) همانند یک افزاره مسیر عبوری[۱۳] میان درخواست‌کننده و سرور احراز هویت عمل می‌کند.

به همین ترتیب، ممکن است سرور احراز هویت در طول برقراری تونل شبکه خصوصی مجازی (VPN)[۱۴] مورد استفاده قرار گیرد. دروازه شبکه خصوصی مجازی همانند یک افزاره مسیر عبوری میان سرویس‌گیرنده شبکه خصوصی مجازی و سرور احراز هویت (محصول) عمل می‌کند. بدون در نظر گرفتن نوع ارتباط (سرور دسترسی شبکه (NAS) خاص)، اجازه دسترسی داده می‌شود و تونل‌های ارتباطی امن فقط درصورتی‌که احراز هویت موفقیت‌آمیز باشد ایجاد می‌شوند.

سرور احراز هویت باید مطابق با RFC 2865 برای ارتباط با سرور دسترسی شبکه (NAS) از خدمت احراز هویت از راه دور کاربران تماس‌گیرنده (RADIUS) پشتیبانی کند، به‌ویژه RADIUS با پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال[۱۵] (EAP-TLS بر روی RADIUS) که در RFC 2865،

---

[۱۰] Wireless Local Area Network (WLAN)

[۱۱] Port-based

[۱۲] authenticator

[۱۳] Pass-through Device

[۱۴] Virtual Private Network (VPN)

RFC 5216 و RFC 2869 مشخص شده‌اند و برای احراز هویت دوطرفه سرور دسترسی شبکه (NAS) و محصول مورد نیاز هستند. تمام ارتباطات پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال (EAP-TLS) میان محصول و سرور دسترسی شبکه (NAS) با استفاده از پروتکل RADIUS منتقل می‌شوند. در برخی سناریوها، استفاده انحصاری از RADIUS برای محافظت از اطلاعات احراز هویت کافی نیست و باید سازوکارهای امنیتی دیگری نیز پشتیبانی شوند تا سرور دسترسی شبکه (NAS) و محصول قادر به برقراری ارتباط امن لایه انتقال با استفاده از تونل امن خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec)[۱۶] یا پروتکل امنیتی IPSec[۱۷] برای حفاظت از پیوند ارتباطی میان خودشان باشند. با این کار اطمینان حاصل می‌شود که خصیصه‌های RADIUS به‌صورت امن منتقل می‌شوند و ترافیک احراز هویت محرمانه باقی می‌ماند.

علاوه بر ارائه ارتباطات امن، محصول باید قابلیت کارکردی برای جداسازی نقش و نظارت سامانه را فراهم آورد. یک نقش مدیریت سیستمی به‌گونه‌ای برقرار می‌شود که تنها مدیران سیستم احراز هویت شده مجاز به دسترسی به سرور احراز هویت برای نصب، پیکربندی و نگهداری می‌باشند. سرور احراز هویت هم از

---

[۱۵] Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)

[۱۶] RadSec یک پروتکل انتقال دیتاگرام RADIUS روی TCP و TLS است.

[۱۷] Internet Protocol Security

سازوکار احراز هویت راه دور و هم از سازوکار احراز هویت محلی برای اجرای ورود به سامانه مدیر سیستم پشتیبانی می‌کند. مدیر سیستم می‌تواند از راه دور با استفاده از ارتباط امن ایجادشده به‌وسیله IPSec، پروتکل پوسته امن (SSH)[۱۸] یا امنیت لایه انتقال (TLS)[۱۹] به محصول دسترسی داشته باشد.

وجود یک سازوکار ممیزی قوی برای اطمینان از مسئولیت‌پذیری در قبال تمام اقدامات مرتبط با امنیت ضروری است. سرور احراز هویت رکوردهای ممیزی را تولید می‌کند و تمام احراز هویت‌های ضروری و رویدادهای سطح سامانه و تمام گزینه‌های پیکربندی را که توسط مدیر سیستم مجاز فراخوانی شده‌اند را ثبت می‌کند. رکوردهای ممیزی در مقابل تغییر یا حذف نامناسب محافظت می‌شوند. محصول با فراهم آوردن امکان تشخیص و نسبت دادن اقدامات مخرب برای مدیران سیستم، امکان بازنگری وقایع ممیزی را محدود به مدیران سیستم مجاز می‌کند.

فرض بر این است که سرور احراز هویت به‌درستی پیاده‌سازی شده و اشتباهات اساسی طراحی در ساختار آن وجود ندارد. فروشنده باید دستورالعمل پیکربندی (مستندات راهنمای اجرایی- روش‌های اجرایی آماده‌سازی (AGD_PRE)، مستندات راهنمای اجرایی–راهنمای کاربر عملیاتی (AGD_OPE)) را برای نصب صحیح ارائه دهد و محصول را برای محیط‌های عملیاتی پشتیبانی شده مدیریت کند.

۲-۱-۱- رمزنگاری

سرور احراز هویت از الگوریتم رمزنگاری استفاده می‌کند که بر اساس خط‌مشی طرح منحصربه‌فرد[۲۰] اعتبارسنجی شده‌اند. تمام توابع رمزنگاری باید با پیاده‌سازی اعتبارسنجی شده مطابق با خط‌مشی طرح منحصربه‌فرد تأیید شده باشد و در حالت تأییدشده اجرا شوند[۲۱].

۲-۱-۲- مدیریتی

---

[۱۸] Secure shell protocol (SSH)

[۱۹] Transport Layer Security (TLS)

[۲۰] در الگوی آمریکا سیاست، استفاده از ماژول تصدیق‌شده استاندارد پردازش اطلاعات فدرال (FIPS) و پیاده‌سازی آن است.

[۲۱] در الگوی آمریکا، لازم است تمام توابع رمزنگاری تأیید شده FIPS، پیاده‌سازی شده در پیمانه اعتبارسنجی شده FIPS و اجرا شده در حالت تأیید شده FIPS باشند.

سرور احراز هویت باید یک نقش مدیریتی برای نصب، پیکربندی و نگهداری محصول ارائه دهد. محصول هم دسترسی احراز هویت شده راه دور و هم دسترسی احراز هویت شده محلی را برای انجام وظایف مدیریتی ارائه می‌دهد. مدیر سیستم می‌تواند با استفاده از ارتباط امن ایجادشده به‌وسیله IPSec، SSH یا TLS، از راه دور به محصول دسترسی داشته باشد. این رابط ممکن است توسط خود محصول ارائه شده باشد، یا در صورتی که محصول یک برنامه کاربردی باشد، توسط سکو زیرینی که محصول بر روی آن مستقر است ارائه شود. اگرچه این بسته الحاقی نیازمند یک نقش مدیریتی است نویسنده هدف امنیتی می‌تواند نقش‌های اجرایی دیگری را بگنجاند تا با استفاده از آن‌ها کارکردهای اجرایی را به نقش‌های اجرایی جداگانه بیشتری تقسیم کند (برای مثال مدیر سیستم رمزنگاری، مدیر سیستم ممیزی). در این صورت، نویسنده هدف امنیتی باید الزامات کارکردی مدیریت امنیت – نقش‌های مدیریت امنیت (FMT_SMR) را اصلاح کند و الزامات مدیریت امنیت کاربردپذیر را برای محدود کردن کارکرد نقش مدیریتی مناسب به‌روزرسانی کند.

مدیران سیستم مجاز، به‌طور صحیح هر دستورالعمل پیکربندی موردنیاز را به همان شکل ارائه شده توسط فروشنده برای پیکربندی ارزیابی شده و دستور داده شده توسط سازمان محلی دنبال می‌کنند. محصول باید علاوه بر کارکردهای تعریف‌شده توسط پروفایل حفاظتی مبنا، توانایی ارائه کارکردهای زیر را داشته باشد:

- توسعه پروتکل RADIUS مطابق با RFC های مناسب،
- برقراری ارتباطات امن با سرور دسترسی شبکه (NAS)،
- اتخاذ تصمیمات احراز هویتی مناسب برای سرور دسترسی شبکه بر اساس محتویات درخواست احراز هویت دریافت شده و داده‌های موجودیت فعال و خط‌مشی‌های احراز هویتی شناخته شده برای محصول،
- تولید ثبت‌های ممیزی از فعالیت سرور احراز هویت مرتبط با امنیت،
- اجازه مدیریت رفتار تابع سرور احراز هویت.

علاوه بر این، اگر محصول ادعای مطابقت با پروفایل حفاظتی برنامه کاربردی (App PP) را به‌عنوان پروفایل حفاظتی مبنا داشته باشد فرض بر این است که کارکردهای زیر توسط محیط عملیاتی مهیا می‌شوند ولی ممکن است توسط خود محصول پیاده‌سازی شده باشد:

- شناسایی و احراز هویت مدیران سیستم خواستار قابلیت مدیریت محصول.
- انتقال ایمن داده‌های ممیزی به یک مخزن داده راه دور.
- ارائه سازوکار به‌روزرسانی امن.
- مهیاکردن توابع رمزنگاری مورد استفاده برای برقراری ارتباطات امن راه دور.
- ذخیره‌سازی ایمن داده اعتبارنامه‌های اجرایی.
- ذخیره‌سازی ایمن داده‌های رمزنگاری مرتبط با امنیت.

فروشنده برای اطمینان از نصب و پیکربندی درست محصول باید دستورالعمل پیکربندی (مستندات راهنمای اجرایی - روش‌های اجرایی آماده‌سازی (AGD_PRE)، مستندات راهنمای اجرایی – راهنمای کاربر عملیاتی (AGD_OPE)) را تهیه کند.

۲-۱-۳-انطباق پروتکل

سرور احراز هویت برای کپسوله‌سازی[۲۲] بسته‌های پروتکل احراز هویت توسعه‌پذیر (EAP)[۲۳] انتقال یافته میان محصول و NAS باید از پروتکل RADIUS (RFC 2865) و RADIUS توسعه‌یافته برای EAP که در RFC 2869 مشخص شده است، پشتیبانی کند. باید از انتقال بسته‌های EAP، RADIUS در تونل شبکه خصوصی مجازی IPSec به همان شکلی که در RFC 4301 مشخص شده است یا از رمزنگاری امنیت لایه انتقال (TLS) بسته‌های RADIUS با استفاده از امنیت خدمت RadSec به همان شکلی که در RFC 6614 به آن اشاره شده است پشتیبانی شود. احراز هویت کلید از قبل به اشتراک گذاشته‌شده برای ارتباط

[۲۲] encapsulation

[۲۳] Extensible Authentication Protocol

امن خدمت RadSec یا تونل IPSec پیاده‌سازی شده است و احراز هویت سیستم رمزنگاری کلید عمومی (RSA)[۲۴] یا الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA)[۲۵] نیز باید پشتیبانی شود. محصول باید برای جلوگیری از به‌کارگیری روش‌های احراز هویتی به‌جز EAP-TLS قابل پیکربندی باشد. دنباله‌های رمز مجاز EAP-TLS در پشتیبانی رمزنگاری احراز هویت توسعه‌پذیر- امنیت لایه انتقال توسعه‌یافته.۱ (FCS_EAP-TLS_EXT.1) مشخص شده‌اند و مدیر سیستم مجاز با توجه به نوع اتصال یا NAS، دنباله‌های رمز مناسب را تنظیم می‌کند. باید از احراز هویت دوطرفه استفاده شود؛ سرور احراز هویت از گواهی ماشین X.509 v3 استفاده می‌کند که توسط یک مرجع صلاحیت‌دار صدور گواهی (CA)[۲۶] مجاز تولید شده‌اند و زوج کلید عمومی/خصوصی را برای احراز هویت خود در طول تبادلات EAP-TLS بکار می‌گیرد. سرور احراز هویت، موجودیت سرویس‌گیرنده را با استفاده از گواهی‌نامه X.509 v3 احراز هویت کرده و گواهی‌نامه‌ها را مطابق با RFC 5280 اعتبارسنجی می‌کند.

۳- تعریف مسائل امنیتی

مسئله امنیتی که سرورهای احراز هویت با آن مواجه هستند، بسط تهدیداتی است که در پروفایل‌های حفاظتی مبنا تعریف شده‌اند. الزامات کارکرد امنیتی که از پروفایل‌های حفاظتی مبنا به دست می‌آیند یا با توجه به شرایط از پروفایل حفاظتی مبنای انتخابی حاصل می‌شوند (بخش‌های ۵-۳ و ۵-۴ را ملاحظه فرمایید) تهدیداتی را مورد توجه قرار می‌دهند که در پروفایل‌های حفاظتی مبنا تعریف شده‌اند. با این وجود قابلیت‌های منحصربه‌فرد سرور احراز هویت تهدیدات اضافی را که در ادامه بیان شده است، تعریف می‌کند.

تهدیدات	توضیحات

[۲۴] RSA از ابتدای نام خانوادگی ران رایوست (Ron Rivest)، ادی شامیر (Adi Shami) و لئونارد ادلمن (Leonard Adleman) تشکیل شده که اولین بار در سال ۱۹۷۷ الگویتم را به‌صورت عمومی توضیح دادند.

[۲۵] Elliptic Curve Digital Signature Algorithm

[۲۶] Certificate Authority

نقطه‌های انتهایی نادرست T.FALSE_ENDPOINTS	محصول درخواست‌های احراز هویت را از مؤلفه‌های NAS محیطی دریافت می‌کند. روشی که به‌وسیله آن محصول پذیرش یا رد درخواست‌های احراز هویت را ابلاغ می‌کند باید با استفاده از پروتکل RADIUS به روش مشخص شده توسط RFC 2865 انتقال یابد به‌طوری که این اطلاعات بتوانند به‌وسیله NAS مستقر در محیط عملیاتی تفسیر شود. علاوه بر این، محصول و NAS باید به‌صورت دوطرفه از هویت یکدیگر اطمینان حاصل کنند. اگر این کار انجام نشود ممکن است محصول به اشتباه داده احراز هویت مرتبط با امنیت را به موجودیتی برگرداند که NAS را جعل کرده است یا ممکن است یک مهاجم بتواند محصول را جعل کرده و سرور دسترسی شبکه (NAS) را به اقدامات نامناسب در پاسخ به درخواست‌های احراز هویت وادارد. تهدید نقطه‌های انتهایی نادرست (T.FALSE_ENDPOINTS) اقدام‌کننده مخربی است که ممکن است محصول یا سرور دسترسی شبکه (NAS) را به‌صورت ساختگی جعل کند تا محصول را وادار به عمل کردن به شیوه‌ای ناامن کند یا داده مرتبط با امنیت را از محصول یا محیط عملیاتی‌اش استخراج کند.
کاربران نامعتبر T.INVALID_USERS	هدف اصلی سرور احراز هویت، احراز هویت کاربران نهایی است که در تلاش برای دسترسی به منابع حفاظت‌شده در محیط عملیاتی هستند؛ بنابراین ارائه قابلیت احراز هویت کاربران معتبر و تضمین عدم احراز هویت کاربران نامعتبر توسط توابع امنیتی هدف ارزیابی ضروری است. تهدید کاربران نامعتبر (T.INVALID_USERS) کاربر مخربی است که ممکن است داده اعتبارنامه نادرست یا دیگر درخواست‌های احراز هویت نامعتبر را که ممکن است توسط محصول پذیرفته یا نادیده گرفته شده است را به‌گونه‌ای عرضه کند که منابع محافظت‌شده در محیط عملیاتی سوژه دسترسی بدون احراز هویت شده باشند.

نگاشت کاملی از مسائل امنیتی در بخش ۷ این پروفایل الحاقی آورده شده است.

۴- اهداف امنیتی

مسائل امنیتی که در بخش قبل توصیف شدند توسط الزامات کارکرد امنیتی اجباری تعریف‌شده در این بسته الحاقی مورد توجه قرار می‌گیرند. الزامات کارکرد امنیتی هم که از پروفایل‌های حفاظتی مبنا به دست می‌آیند برای مورد توجه قرار دادن تهدیداتی مورد استفاده قرار می‌گیرند که در آن پروفایل‌های حفاظتی تعریف شده‌اند. اگر محصول ادعای انطباق با پروفایل حفاظتی برنامه کاربردی (App PP) مبنا را داشته باشد، تهدیدات تعریف‌شده برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا را علاوه بر تهدیداتی که به‌صورت خاص برای پروفایل حفاظتی برنامه کاربردی (App PP) تعریف شده است را نیز برآورده خواهد کرد، این کار از طریق قابلیت‌های کارکردی خود یا از طریق امنیتی که فرض می‌شود توسط سکو زیرین فراهم شده باشد صورت می‌گیرد (بخش ۵-۴-۲ را برای راهنمایی در این مورد ببینید). اگر محصول ادعای انطباق با پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) مبنا را داشته باشد مرز محصول شامل سکو زیرین است و در نتیجه انتظار نمی‌رود که الزامات پروفایل حفاظتی برنامه کاربردی (App PP) اجرایی شوند که بر روی تعاملات برنامه کاربردی با سکو محیطی‌اش متمرکز هستند.

نکته: در هرکدام از زیربخش‌های زیر اهداف امنیتی خاص شناسایی شده‌اند (با O بیان شده‌اند) و با الزامات کارکرد امنیتی مرتبط که سازوکارهایی برای برآورده ساختن اهداف فراهم می‌کنند، منطبق هستند.

هدف امنیتی	توضیحات

کاربری پروتکل استاندارد شده O.Deep_Inspection	برای اطمینان از اینکه محصول می‌تواند به‌درستی کاربران معتبر را احراز هویت کند، محصول باید پروتکل RADIUS را مطابق با مشخصات پیاده‌سازی کند. این نه تنها شامل ساماندهی صحیح درخواست‌های احراز هویت است بلکه درستی‌سنجی، صحت و یکپارچگی بسته‌هایی را که درخواست‌ها را در برمی‌گیرند نیز شامل می‌شود. نقص در انجام این کار، منجر به عدم تضمین کارکرد مناسب محصول می‌شود. هدف امنیتی کاربری پروتکل استاندارد RADIUS (O.RADIUSCOMPLIANT) با الزام کارکرد امنیتی ارتباطات - اثبات مبدأ انتخابی (FCO_NRR.1)، الزام کارکرد امنیتی پشتیبانی رمزنگاری RADIUS توسعه‌یافته (FCS_RADIUS_EXT.1) و الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته (FCS_RADSEC_EXT.1) در ارتباط است: (O.RADIUSCOMPLIANT->FCO_NRO.1, FCO_NRR.1, FCS_RADIUS_EXT.1, FCS_RADSEC_EXT.1)
احراز هویت دوطرفه O.Failure	برای کاهش ریسک جعل هویت محصول یا NAS که درخواست‌های احراز هویت را دریافت می‌کنند، انتظار می‌رود محصول اقداماتی را پیاده‌سازی کند که اجازه شناسایی و احراز هویت NAS را می‌دهد و اطلاعاتی را در اختیار NAS قرار دهد که احراز هویت دوطرفه را امکان‌پذیر می‌کند. هدف امنیتی احراز هویت دوطرفه محصول و NAS با الزام کارکرد امنیتی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال (EAP-TLS) توسعه‌یافته (FCS_EAP-TLS_EXT.1)، الزام کارکرد امنیتی شناسایی و احراز هویت ترکیب کلید از قبل به اشتراک گذاشته‌شده توسعه‌یافته (FIA_PSK_EXT.1) و الزام کارکرد امنیتی مسیر امن – کانال امن درونی محصول (FTP_ITC.1) در ارتباط است: (O.TRUSTEDNAS -> FCS_EAP-TLS_EXT.1, FIA_PSK_EXT.1, FTP_ITC.1)

احراز هویت کاربر احراز معتبر O.Hidden Data	محصول باید بر اساس هویت و داده اعتبارنامه دریافتی بتواند تصمیمات احراز هویت را اتخاذ کند. محصول ممکن است بر اساس داده‌های متنی متفاوت مثل زمان یا روز اقدام، نوع اعتبارنامه استفاده‌شده یا دیگر خصیصه‌های مرتبط اختصاص داده شده به موجودیت فعال، نتایج احراز هویت متفاوتی را بازگرداند. این داده‌های خصیصه‌ای ممکن است توسط محصول حفظ و نگهداری شوند یا محصول توانایی ارتباط با یک مخزن در محیط عملیاتی که داده در آن نگهداری می‌شود، فراهم آورد. هدف امنیتی احراز هویت کاربر معتبر با الزام کارکرد امنیتی شناسایی و احراز هویت-ساماندهی شکست احراز هویت (FIA_AFL.1)، الزام کارکرد امنیتی شناسایی و احراز هویت-احراز هویت مجدد (FIA_UAU.6) و الزام کارکرد امنیتی دسترسی به محصول–برقراری نشست محصول (FTA_TSE.1) در ارتباط است: (O.USERAUTH -> FIA_AFL.1, FIA_UAU.6, FTA_TSE.1)

۵- الزامات کارکرد امنیتی

این بخش الزامات کارکرد امنیتی[۲۷] محصول را مشخص می‌کند و اقدامات تضمینی که ارزیاب باید انجام دهد، در بخش ۶، مربوط به الزامات تضمین امنیت مشخص شده‌است.

۵-۱- قراردادها

با وجود اینکه الزامات کارکرد امنیتی توسعه‌یافته به این بسته اضافه شده است، ولی به روشی انعطاف‌پذیر تعریف شده‌اند که قابلیت استفاده در این بسته الحاقی و دیگر بسته‌ها یا پروفایل‌های حفاظتی را داشته باشند و چنین عملیاتی در محتوای این بسته الحاقی انجام می‌شود.

[۲۷] Security Functional Requirement

معیار مشترک عملیات بر روی الزامات کارکرد امنیتی را چنین تعریف می‌کند: اختصاص‌ها، انتخاب‌ها و اختصاص‌هایی درون انتخاب‌ها و پالایش‌ها. این سند از قراردادهای نگارشی زیر برای شناسایی عملیات تعریف‌شده توسط معیار مشترک استفاده می‌کند.

- اختصاص: با متن مورب[۲۸] نشان داده شده و با «اختصاص:» شروع می‌شود.
- پالایش انجام شده توسط نویسنده پروفایل حفاظتی: با کلمه «پالایش» به‌صورت **متن پررنگ** پس از شماره عنصر با متن اضافی **پررنگ** و حذف با خط‌خوردگی، در صورت لزوم نمایش داده می‌شود؛
- انتخاب: با متن زیر خط‌دار[۲۹] نشان داده‌شده و با «انتخاب:» شروع می‌شود.
- اختصاص در داخل انتخاب: با متن *مورب و زیر خط‌دار*[۳۰] مشخص می‌شود.
- تکرار: با تعداد تکرار در داخل پرانتز نشان داده می‌شود. برای مثال (۱)، (۲)، (۳).

در ضمن همه عملیات اختصاص و انتخاب با براکت نشان داده می‌شوند. در برخی موارد بسته الحاقی مستلزم آن است که عملیات انتخاب و یا اختصاص با جملات خاصی تکمیل شوند. زمانی که این اتفاق روی می‌دهد قالب تعریف‌شده برای عملیات به‌جز برای کلمات «انتخاب:» و «اختصاص:» که حذف شده است، حفظ می‌شود.

۵-۲- جهت‌گیری الزامات کارکرد امنیتی بسته الحاقی

[۲۸] Italicized text

[۲۹] Underlined text

[۳۰] Italicized and underlined text

این بخش الزامات کارکرد امنیتی را توصیف می‌کند که باید توسط هر محصول که ادعای انطباق با این بسته الحاقی دارد تأمین شوند. این الزامات کارکرد امنیتی باید بدون در نظر گرفتن اینکه پروفایل حفاظتی مبنا، پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) یا پروفایل حفاظتی برنامه کاربردی (App PP) هستند مطرح شوند.

جدول ۱ الزامات کارکرد امنیتی بسته الحاقی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**اثبات مبدأ انتخابی[۳۱] ۱**	FCO_NRO.1.1
۲	**اثبات مبدأ انتخابی ۲**	FCO_NRO.1.2
۳	**اثبات مبدأ انتخابی ۳**	FCO_NRO.1.3
۴	**اثبات دریافت انتخابی (اعلام وصول)۱**	FCO_NRR.1.1
۵	**اثبات دریافت انتخابی (اعلام وصول)۲**	FCO_NRR.1.2
۶	**اثبات دریافت انتخابی (اعلام وصول)۳**	FCO_NRR.1.3
۷	**امنیت لایه انتقال-پروتکل الحاق هویت توسعه‌پذیر ۱**	FCS_EAP-TLS_EXT.1.1
۸	**امنیت لایه انتقال-پروتکل الحاق هویت توسعه‌پذیر ۲**	FCS_EAP-TLS_EXT.1.2
۹	**امنیت لایه انتقال-پروتکل الحاق هویت توسعه‌پذیر ۳**	FCS_EAP-TLS_EXT.1.3
۱۰	**امنیت لایه انتقال-پروتکل الحاق هویت توسعه‌پذیر ۴**	FCS_EAP-TLS_EXT.1.4
۱۱	**امنیت لایه انتقال-پروتکل الحاق هویت توسعه‌پذیر ۵**	FCS_EAP-TLS_EXT.1.5
۱۲	**امنیت لایه انتقال-پروتکل الحاق هویت توسعه‌پذیر ۶**	FCS_EAP-TLS_EXT.1.6
۱۳	**RADIUS ۱**	FCS_RADIUS_EXT.1.1
۱۴	**RADIUS ۲**	FCS_RADIUS_EXT.1.2

[۳۱] Selective Proof of Origin

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۵	**۳ RADIUS**	FCS_RADIUS_EXT.1.3
۱۶	**ترکیب کلید از قبل به اشتراک گذاشته‌شده ۱**	FIA_PSK_EXT.1.1
۱۷	**ترکیب کلید از قبل به اشتراک گذاشته‌شده ۲**	FIA_PSK_EXT.1.2
۱۸	**برقراری نشست محصول ۱**	FTA_TSE.1.1
۱۹	**کانال امن درون محصول ۱**	FTP_ITC.1.1
۲۰	**کانال امن درون محصول ۲**	FTP_ITC.1.2
۲۱	**کانال امن درون محصول ۳**	FTP_ITC.1.3

۵-۲-۱-ارتباطات

شماره الزام	نام الزام
۱	**اثبات مبدأ انتخابی ۱**
محصول باید قادر به تولید شواهدی از مبدأ برای [بسته‌های Access-Request RADIUS] انتقال‌یافته هنگام درخواست [گیرنده پیام] باشد. **نکته کاربردی ۱:** هدف از این الزام ایجاد توانایی در محصول برای اعتبارسنجی NAS و جلوگیری از استراق سمع این مؤلفه است. در این مورد محصول گیرنده -Access Request منتقل شده است و باید توانایی شناسایی جایی را که این درخواست از آن دریافت شده است را داشته باشد	
۲	**اثبات مبدأ انتخابی ۲**
محصول باید بتواند میان [احراز هویت کننده پیام] از مبدأ اطلاعات و [Access-Request] اطلاعات که شواهد در آن صادق باشد ارتباط برقرار کند. **نکته کاربردی ۲:** هدف از این الزام ایجاد توانایی در محصول برای اعتبارسنجی اصالت‌سنجی NAS به‌ویژه از طریق بررسی احراز هویت کننده پیام است که در قسمتی با	

استفاده از یک راز مشترک معلوم برای محصول و NAS مورد پردازش قرار می‌گیرد. این رفتار در RFC 3579 تعریف شده است.	
اثبات مبدأ انتخابی ۳	**۳**
محصول باید توانایی بررسی شواهد منبع را از اطلاعات [گیرنده پیام] داده شده [شواهدی از اطلاعات مبدأ اطلاعات در بسته درخواست دسترسی به روشی سازگار با RFC 2865 سازگار ارائه شده است] داشته باشد.	
اثبات دریافت انتخابی ۱	**۴**
محصول باید قادر به تولید شواهدی از دریافت برای [بسته‌های Access-Request RADIUS] دریافت شده هنگام درخواست [صادر کننده پیام] باشد. **نکته کاربردی ۳:** هدف از این الزام این است که محصول بتواند پاسخ معتبری پس از دریافت Access-Request، به NAS برگرداند.	
اثبات دریافت انتخابی ۲	**۵**
محصول باید میان [شناسه، احراز هویت کننده پاسخ] از دریافت‌کننده اطلاعات و [بسته پاسخ] از اطلاعاتی که در آن شواهد صدق می‌کند ارتباط برقرار کند. **نکته کاربردی ۴:** هدف از این الزام این است که نویسنده هدف امنیتی فهرستی از اطلاعات تأمین شده توسط محصول در پاسخ به بسته‌های (Access-Accept، Access-Request یا Access-Challenge) را تهیه کند که نشان‌دهنده موارد زیر است: • Access-Request که باید به آن‌ها پاسخ داده شود؛ • احرازهویت‌کننده‌ی پاسخ که بر اساس قسمتی از راز مشترک معلوم برای محصول و NAS، محصول را به عنوان دریافت‌کننده معتبر Access-Request اصلی شناسایی می‌کند. این رفتار در RFC 2865 تعریف شده است.	
اثبات دریافت انتخابی ۳	**۶**

محصول باید توانایی بررسی شواهد دریافت اطلاعات [صادرکننده پیام] داده شده [اختصاص: محدودیت‌هایی بر روی مدارک دریافت] را داشته باشد.

۵-۲-۲- پشتیبانی رمزنگاری

شماره الزام	نام الزام
۷	**پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال ۱**
محصول باید پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال (EAP-TLS) را به همان شکلی که در RFC 5216 مشخص شده است و با [انتخاب: امنیت لایه انتقال (RFC 4346)(TLS 1.1، امنیت لایه انتقال (RFC 5246) (TLS 1.2)] پیاده‌سازی کند و دیگر نسخه‌های امنیت لایه انتقال (TLS) را نباید پیاده‌سازی کرد و دنباله رمز زیر را پشتیبانی کند. دنباله رمز اجباری مطابق با RFC 3268: • TLS_RSA_WITH_AES_128_CBC_SHA دنباله‌های رمز اختیاری: [انتخاب: • TLS_RSA_WITH_AES_256_CBC_SHA. • TLS_DHE_RSA_WITH_AES_128_CBC_SHA. • TLS_DHE_RSA_WITH_AES_256_CBC_SHA. • TLS_RSA_WITH_AES_128_CBC_SHA256 که در RFC 5246 تعریف شده است. • TLS_RSA_WITH_AES_256_CBC_ SHA256 که در RFC 5246 تعریف شده است.	

- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 که در RFC 5246 تعریف شده است.
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 که در RFC 5246 تعریف شده است.
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 که در RFC 5289 تعریف شده است.
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 که در RFC 5289 تعریف شده است.
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 که در RFC 5430 تعریف شده است.
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 که RFC 5430 تعریف شده است.
- هیچ دنباله رمز دیگری].

نکته کاربردی ۵: نکته کاربردی: دنباله رمزهایی که باید در پیکربندی ارزیابی شده آزموده شود با الزام محدود شده‌اند. نویسنده هدف امنیتی باید دنباله رمزهای اختیاری مورد پشتیبانی را انتخاب کند؛ اگر هیچ‌یک از دنباله‌های رمز موجود در فهرست اجباری پشتیبانی نشوند باید «هیچ » انتخاب شود. محدود کردن دنباله‌های رمز که می‌تواند در یک پیکربندی ارزیابی شده اجرایی روی سرور در محیط آزمون استفاده شود، ضروری است. الگوریتم‌های مجموعه B که در بالا به آن‌ها اشاره شده است (RFC 6460) الگوریتم‌هایی هستند که برای پیاده‌سازی ترجیح داده شده‌اند. TLS_RSA_WITH_AES_128_CBC_SHA برای اطمینان از انطباق با RFC 5246 مورد نیاز است.

اگر دنباله رمز منحنی-بیضوی انتخاب شود، الزام کارکرد امنیتی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال توسعه‌یافته۱,۷. (FCS_EAP-TLS_EXT.1.7) که در پیوست ۲ آورده شده است باید در هدف امنیتی آورده شود.

پروتکل امنیت لایه انتقال (TLS 1.2) بیشتر مورد استفاده قرار می‌گیرد. امنیت لایه انتقال (TLS 1.1) افزونه‌های ضروری برای تضمین ارتباط با استحکام امنیتی ۱۱۲ بیتی یا بهتر از آن را ندارد.

امنیت لایه انتقال (TLS 1.2) که برای EAP-TLS محصولات مورد ارزیابی قرار گرفته بعد از سه‌ماهه سوم ۲۰۱۵ مورد نیاز است. این الزامات در بازبینی جدید به‌عنوان نسخه جدید امنیت لایه انتقال (TLS) توسط IETF استاندارد می‌شود.

۸	پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال ۲

محصول باید مقادیر تصادفی مورد استفاده در تبادلات EAP-TLS را با استفاده از تولید کننده بیت تصادفی (RBG) معین‌شده در الزام کارکرد امنیتی پشتیبانی رمزنگاری تولید بیت تصادفی توسعه‌یافته.۱ (FCS_RBG_EXT.1) تولید کند.	
پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال ۳	**۹**
محصول باید گواهینامه‌ای را از سرویس گیرنده، خواستار احراز هویت سرویس گیرنده درخواست کند.	
پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال ۴	**۱۰**
محصول باید بررسی کند که گواهینامه ارائه‌شده از جانب سرویس گیرنده شامل هدف احراز هویت سرویس گیرنده (OID 1.3.6.1.5.5.7.3.2) در فیلد کاربرد کلید (KeyUsage field) توسعه‌یافته است و بیت توافق کلید[۳۲] در فیلد کاربرد کلید (OID 2.5.29.15.4) تنظیم شده است.	
پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال ۵	**۱۱**
محصول باید از نسخه ۳ گواهی‌نامه X509 به شکلی که در الزام کارکرد امنیتی شناسایی و احراز هویت گواهی X509 توسعه‌یافته.۱ (FIA_X509_EXT.1) مشخص شده است استفاده کند.	
پروتکل احراز هویت توسعه‌پذیر-امنیت لایه انتقال ۶	**۱۲**
محصول باید به مدیر سیستم مجاز اجازه دهد تا فهرستی از مجموعه الگوریتم‌هایی که ممکن است در طول تبادلات EAP-TLS پیشنهادشده و پذیرفته شود را پیکربندی کند. **نکته کاربردی ۶:** الزام کارکرد امنیتی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال (EAP-TLS) توسعه‌یافته.۱,۴ (FCS_EAP-TLS_EXT.1.4) مستلزم آن است که به بیت توافق کلید در پشتیبانی. از دنباله رمزهای اجباری دیفی-هلمن تنظیم شود. اگر نویسنده هدف امنیتی استفاده از یک دنباله رمز اختیاری رایوست-شامیر-ادلمن (RSA) را انتخاب کند، این مؤلفه باید تکرار شود و بیت کلید توافق "key agreement bit" جایگزین بیت کلید رمزگذاری "encipherment bit key" شود.	

[۳۲] Key Agreement

۱۳	**خدمت احراز هویت از راه دور کاربران تماس‌گیرنده (RADIUS) ۱**
محصول باید پروتکل RADIUS را به همان شکلی که در RFC 2865 مشخص شده است برای برقراری ارتباط با NAS به کار گیرد.	
۱۴	**خدمت احراز هویت از راه دور کاربران تماس‌گیرنده (RADIUS) ۲**
محصول باید EAP کپسوله‌شده در RADIUS را به همان شکل مشخص شده در RFC 3579 پیاده‌سازی کند.	
۱۵	**خدمت احراز هویت از راه دور کاربران تماس‌گیرنده (RADIUS) ۳**
بسط RADIUS برای EAP (RFC 2869) باید به همان شکل مشخص شده در RFC 5216 استفاده از EAP-TLS را پشتیبانی کند. **نکته کاربردی ۷:** نویسنده هدف امنیتی باید توضیح دهد که چگونه محصول شرایطی را تعیین می‌کند که در این شرایط صدور پاسخ به چالش-دسترسی NAS جدا از موارد مورد نیاز پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال (EAP-TLS) ضروری است.	

۵-۲-۳- شناسایی و احراز هویت

شماره الزام	نام الزام
۱۶	**ترکیب کلید از قبل به اشتراک گذاشته شده ۱**
محصول باید بتواند از کلیدهای از قبل به اشتراک گذاشته شده برای [انتخاب: IPsec، امنیت خدمت RadSec] و [RADIUS] استفاده کند. **نکته کاربردی ۸:** انتخاب IPsec و RasSec باید با انتخاب الزام کارکرد امنیتی مسیر امن – کانال امن درونی محصول (FTP_ITC.1) مطابقت داشته باشد. کلید از قبل به اشتراک گذاشته مورداستفاده برای RADIUS راز به اشتراک گذاشته شده RADIUS است.	
۱۷	**ترکیب کلید از قبل به اشتراک گذاشته شده ۲**
محصول باید بتواند کلیدهای از قبل به اشتراک گذاشته متنی را بپذیرند که:	

– ۲ کاراکتر دارند و [انتخاب: [اختصاص: *دیگر طول‌های پشتیبانی شده*]، هیچ طول دیگری]؛ متشکل از هر ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص (شامل: «!»، «@»، «#»، «$»، «٪»، «^»، «&»، «*»، «(«و»)») باشد.

۵-۲-۴- دسترسی محصول

شماره الزام	نام الزام
۱۸	**برقراری نشست محصول۱**
محصول باید قادر به رد برقراری نشست کاربر بر اساس [اختصاص: خصیصه‌ها] باشد. **نکته کاربردی ۹:** نویسنده هدف امنیتی باید همه شرایطی را که ممکن است باعث عدم پذیرش درخواست احراز هویت کاربر شوند توضیح دهد. تمام محصولات سازگار با توجه به اعتبارنامه‌های نامعتبر درخواست احراز هویت را رد خواهند کرد ولی ممکن است بسته به قابلیت‌های سازوکار احراز هویت محصول، محدودیت‌های اضافه‌تری همچون حساب‌های کاربری به تعلیق درآمده یا محدودیت‌های زمانی روزانه را اعمال کنند.	

۵-۲-۵- مسیر/کانال امن

شماره الزام	نام الزام
۱۹	**کانال امن درونی محصول ۱**
محصول باید کانال ارتباطی [انتخاب: IPsec، امنیت خدمت RadSec] میان خود و یک NAS را ارائه دهد که به‌صورت منطقی از دیگر کانال‌های ارتباطی جدا است و شناسایی مطمئنی از نقاط انتهایی خود و محافظت از داده کانال در مقابل تغییر یا افشاء داده کانال فراهم می‌کند.	
۲۰	**کانال امن درونی محصول ۲**
محصول باید به [محصول یا NAS] اجازه دهد تا ارتباط را از طریق کانال امن آغاز کند.	

۲۱	کانال امن درونی محصول ۳
محصول باید برای [پاسخگویی به پیام‌های Access-Request RADIUS دریافت شده از NAS] ارتباط را از طریق کانال امن آغاز کند. **نکته کاربردی ۱۰:** اگر بسته الحاقی برای توسعه پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) استفاده شود، الزام کارکرد امنیتی مسیر / کانال امن - کانال امن درونی محصول (FTP_ITC.1) باید در پروفایل حفاظتی مبنا وجود داشته باشد. در این مورد انتظار می‌رود نویسنده هدف امنیتی یک عملیات تکراری را برای هر دو نمونه الزام کارکرد امنیتی مسیر/ کانال امن - کانال امن درونی محصول (FTP_ITC.1) به‌کار برد تا نام‌های الزامات کارکرد امنیتی همچنان یکتا بمانند. در این صورت، انتظار می‌رود ارزیاب اقدامات تضمینی را برای هر تکرار الزام کارکرد امنیتی اعمال کند.	

۵-۳- جهت‌گیری الزامات کارکرد امنیتی پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)

اگر این بسته الحاقی، پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) را توسعه داده باشد، انتظار می‌رود سرور احراز هویت به توابع امنیتی پیاده‌سازی شده توسط افزاره شبکه به‌عنوان یک کل متکی باشد و بر اساس پروفایل حفاظتی مبنا ارزیابی شود. اگر محصول ادعای انطباق با این بسته الحاقی را داشته باشد که از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) به‌عنوان پروفایل حفاظتی مبنای ادعاشده استفاده می‌کند، بخش‌های زیر هر تغییری که نویسنده هدف امنیتی باید در الزامات کارکرد امنیتی تعریف‌شده در پروفایل حفاظتی مبنا و آنچه در بخش ۵-۲ اجباری شده است ایجاد کند را توصیف می‌کند.

جدول ۲ الزامات کارکرد امنیتی پروفایل حفاظتی مشترک افزاره شبکه

شماره	نام کلاس	الزام	نام الزام
۱	الزامات اختیاری	ادعای الزامات برای این بسته الحاقی اجباری نیست.	ادعای آن‌ها، برای این بسته الحاقی اجباری نیست.
۲	ممیزی امنیتی	FAU_GEN.1	تولید داده ممیزی
۳	شناسایی و احراز	FIA_AFL.1	ساماندهی شکست احراز هویت
۴	مدیریت امنیت	FMT_SMF.1	مشخصات توابع مدیریت

۵-۳-۱-گنجاندن الزامات اختیاری

برای اینکه محصول تمام وابستگی‌های ضروری را برآورده کند، پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) ادعا شده باید تمام الزامات مبنا را از آن پروفایل حفاظتی و هر الزام مبتنی بر انتخاب مرتبط با پروتکل مورداستفاده توسط محصول را در برگیرد. اگر الزامات کارکرد امنیتی اختیاری دیگری از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) برای محصول کاربردپذیر باشد، این الزامات باید ادعا شوند ولی برای این بسته الحاقی اجباری نیستند.

۵-۳-۲- ممیزی امنیتی

شماره الزام	نام الزام
۲۲	**تولید داده ممیزی ۱**

نکته کاربردی ۱۱: هیچ الزام کارکردی امنیتی اضافه‌ای برای ممیزی امنیتی وجود ندارد. با این وجود رویدادهای قابل ممیزی اضافه‌ای وجود دارند که برای گسترش الزامات کارکرد امنیتی ممیزی امنیتی - تولید داده ممیزی (FAU_GEN.1) موجود در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) وجود دارند. برای مثال رویدادهای موجود در جدول زیر باید با موارد اشاره‌شده برای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) در زمینه‌های منطبق بر اهداف امنیتی ترکیب شوند.

رویدادهای قابل ممیزی:

الزام	رویداد قابل ممیزی	محتواهای ثبت ممیزی اضافی
FCO_NRO.1	درخواست سرویس گیرنده برای چیزی که محصول راز به اشتراک گذاشته شده‌ای با آن ندارد.	هویت سرویس گیرنده، محتویات پاسخ EAP (در صورت وجود)
FCO_NRR.1	هیچ	هیچ
FCS_EAP-TLS_EXT.1	شکست پروتکل، برقراری یک نشست TLS	اگر شکست اتفاق بیافتد، یک دلیل توصیفی برای شکست ثبت شود

FCS_RADIUS_EXT.1	شکست پروتکل، موفقیت/ شکست احراز هویت	اگر شکست اتفاق بیافتد، یک دلیل توصیفی برای شکست ثبت شود	
FCS_RADSEC_EXT.1 (مبتنی بر انتخاب)	شکست در برقراری نشست RadSec	دلایل شکست	
FIA_AFL.1	رسیدن به حد آستانه تلاش‌های احراز هویت ناموفق. غیرفعال کردن یک حساب کاربری به خاطر رسیدن به حد آستانه	هویت کاربر ادعا شده در تلاش برای کسب دسترسی یا پروتکل اینترنتی (IP) که تلاش از آنجا ناشی می‌شود.	
FIA_PSK_EXT.1	هیچ	هیچ	
(اختیاری) FIA_UAU.6	تمام استفاده‌ها از سازوکار احراز هویت	مبدأ تلاش (به‌عنوان‌مثال، نشانی پروتکل اینترنت (IP address))	
FTA_TSE.1	انکار برقراری نشست ناشی از سازوکار برقراری نشست	دلایل انکار، مبدأ برقراری تلاش	
FTP_ITC.1	شروع کانال امن، خاتمه دادن به کانال امن، شکست توابع کانال امن	شناسایی آغاز کننده و هدف از تلاش برای برقراری کانال امن شکست‌خورده	

۵-۳-۳- شناسایی و احراز هویت

شماره الزام	نام الزام
۲۳	**ساماندهی شکست احراز هویت ۱**
محصول باید تشخیص دهد که تلاشهای پی‌درپی احراز هویت ناموفق مربوط به مدیران سیستم از راه دور اتفاق می‌افتد و آن را با یک عدد مثبت قابل تنظیم توسط مدیر سیستم تنظیم کند.	
۲۴	**ساماندهی شکست احراز هویت ۲**

زمانی که به تعداد تعریف شده تلاش برای احراز هویت ناموفق رسید، محصول باید [انتخاب، یکی را انتخاب کند: جلوگیری از احراز هویت موفق مدیر سیستم متخلف از راه دور تا [اختصاص: اقدام] توسط یک مدیر سیستم محلی اتخاذ شود؛ جلوگیری از احراز هویت موفق مدیر سیستم متخلف راه دور تا یک بازه زمانی تعریف‌شده توسط مدیر سیستم سپری شود].

نکته کاربردی ۱۲: این الزام برای یک مدیر سیستم در کنسول محلی به کار نمی‌رود، چون مضمونی برای قفل‌کردن حساب کاربری یک مدیر سیستم محلی در این حالت ایجاد نمی‌کند. این موضوع می‌تواند از طریق درخواست یک حساب کاربری جدا برای مدیران سیستم محلی یا داشتن پیاده‌سازی سازوکار احراز هویت که تلاش‌های ورود به سیستم محلی و از راه دور را تشخیص دهد مورد رسیدگی قرار گیرد. «اقدام» اتخاذشده توسط مدیر سیستم محلی خاص پیاده‌سازی بوده و ممکن است در راهنمای مدیران سیستم تعریف شود (برای مثال، تنظیم مجدد کلمه عبور یا تنظیم مجدد قفل). نویسنده هدف امنیتی بسته به نحوه‌ای که محصول این سامان دهنده را پیاده‌سازی کرده است یکی از گزینه‌ها را برای ساماندهی شکست در احراز هویت انتخاب می‌کند.

۵-۳-۴- مدیریت امنیت

شماره الزام	نام الزام
۲۵	**مشخصات توابع مدیریت ۱**

نکته کاربردی ۱۳: الزامات کارکرد امنیتی اضافه‌ای برای مدیریت امنیت وجود ندارد. با این وجود، کارکرد مدیریتی دیگری نیز هستند که برای توسعه الزام کارکرد امنیتی مدیریت امنیت - مشخصات توابع مدیریت (FMT_SMF.1) مربوط به الزامات کارکرد امنیتی موجود در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) به کار می‌روند. به همین ترتیب، رویدادهای زیر باید برای انطباق اهداف امنیتی با رویدادهای پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) ترکیب شوند.

- توانایی برای تنظیم راز به اشتراک گذاشته شده RADIUS
- توانایی برای تعریف NAS مجاز
- توانایی برای فعال کردن، غیرفعال کردن، تعیین و تغییر رفتار تمام محصول که در این بسته الحاقی برای مدیر سیستم شناسایی شده‌اند.

- [انتخاب: توانایی برای تنظیم و پیکربندی کارکرد IPsec،
هیچ تابع دیگری]

۵-۴- جهت‌گیری الزامات کارکرد امنیت برای پروفایل حفاظتی برنامه کاربردی (App PP)

اگر این بسته الحاقی پروفایل حفاظتی برنامه کاربردی (App PP) را گسترش دهد انتظار می‌رود سرور احراز هویت بر توابع امنیتی. تکیه کند که برای همه برنامه‌های کاربردی عملی هستند (و یا توابعی که توسط سکو زیرین که برنامه کاربردی بر روی آن مستقر شده است فراهم شده‌اند) و بر اساس پروفایل حفاظتی مبنا ارزیابی شود. اگر محصول، ادعای انطباق با این بسته الحاقی را داشته باشد و از پروفایل حفاظتی برنامه کاربردی (App PP) به‌عنوان پروفایل حفاظتی مبنا استفاده کند، بخش‌های زیر تغییراتی را توضیح می‌دهد که نویسنده هدف امنیتی باید برای الزامات کارکرد امنیتی تعریف‌شده در پروفایل حفاظتی مبنا علاوه بر آنچه در بخش ۵-۲ اجباری شده است ایجاد کند.

جدول ۳: الزامات کارکرد امنیت پروفایل حفاظتی برنامه کاربردی

شماره	نام کلاس	الزام	نام الزام
۱	الزامات اختیاری (پشتیبانی رمزنگاری و شناسایی احراز هویت)	FCS_CKM_EXT.1	الزام کارکردی پشتیبانی رمزنگار – مدیریت کلید رمزنگاری الحاقی
		FIA_X509_EXT.1	الزام کارکرد امنیتی شناسایی و احراز هویت – گواهی‌نامه 509 توسعه‌یافته
۲	الزامات کارکردی امنیت جهت ارائه قابلیت‌های سکو زیرین	عنوان کامل این الزامات در جدول ۵ آمده است.	عنوان کامل این الزامات قابلیت‌هایی که ارائه می‌دهند، در جدول ۵ آمده است.
۳	ممیزی امنیتی	FAU_GEN.1	تولید داده ممیزی
۴	مدیریت امنیت	FMT_SMF.1	مشخصات توابع مدیریت
		FMT_SMR.2	محدودیت‌هایی بر روی نقش‌های امنیتی
۵	محافظت از محصول	FPT_TST_EXT.1	آزمون محصول توسعه‌یافته

۵-۴-۱-گنجاندن الزامات اختیاری

برای اینکه محصول تمام وابستگی‌های ضروری را برآورده سازد، پروفایل حفاظتی برنامه کاربردی (App PP) ادعا شده باید شامل تمام الزامات مبنا و نیز الزامات کارکرد امنیتی مبتنی بر انتخاب زیر باشد.

- الزام کارکردی پشتیبانی رمزنگار – مدیریت کلید رمزنگاری الحاقی (FCS_CKM_EXT.1)
- الزام کارکرد امنیتی شناسایی و احراز هویت – گواهی‌نامه 509 توسعه‌یافته.۱ (FIA_X509_EXT.1)

حتی اگر انتخاب‌های مربوط در الزامات کارکرد امنیتی پروفایل حفاظتی برنامه کاربردی (App PP) مبنا وجود نداشته باشند، گنجاندن این الزامات کارکرد امنیتی ضروری است چراکه الزامات کارکردی خاص این بسته الحاقی، این توابع را به عنوان وابستگی دارد. اگر الزامات کارکرد امنیتی اختیاری، مبتنی بر انتخاب یا الزامات هدف از این پروفایل حفاظتی برنامه کاربردی (App PP) برای محصول کاربردپذیر باشد باید ادعا شوند ولی برای این بسته الحاقی اجباری نیستند.

۵-۴-۲- قابلیت‌های سکو زیرین

به عنوان الحاقیه‌ای بر پروفایل حفاظتی برنامه کاربردی (App PP)، فرض شده است که محصول مدعی انطباق با این بسته الحاقی برای تعدادی از توابع امنیتی تعریف‌شده در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) به سکو زیرین خود متکی هستند چرا که این‌ها توابعی نیستند که به‌صورت عمومی توسط برنامه‌های نرم‌افزاری در دسترس باشند. هر چند یک حالت می‌تواند این باشد که محصول به‌جای اینکه به‌طور کامل به محیط عملیاتی خودش وابسته باشد، خود این قابلیت‌ها را ارائه دهد. در این موارد، انتظار می‌رود نویسنده هدف امنیتی الزامات کارکرد امنیتی مرتبط را از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) درخواست کند که نحوه اجرای این قابلیت‌های کارکردی را توضیح می‌دهد. جدول زیر فهرستی از موارد مرتبط و الزامات کارکرد امنیتی که برای مورد توجه قرار دادن آن‌ها باید ادعا شوند را ارائه می‌دهد. توجه داشته باشید به‌جز موارد مشخص شده، تعریف الزامات کارکرد امنیتی و اقدامات تضمین مرتبط باید مستقیماً از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) گرفته شوند.

جدول ۴ الزامات کارکردی امنیت

قابلیت ارائه‌شده توسط محصول	الزامات کارکرد امنیتی که باید گنجانده شوند
سازوکار احراز هویت مشخص که از سکو زیرین به ارث برده نشده است.	FIA_AFL.1 (بخش ۵-۳-۳-۱ را ببینید)
	FIA_PMG_EXT.1
	FIA_UIA_EXT.1
	FIA_UAU_EXT.2
	FIA_UAU.7
	FTA_TAB.1
توانایی انتقال داده ممیزی به منبع ذخیره‌سازی دور با استفاده از سازوکار ورود به سیستم که توسط سکو زیرین فراهم نشده است.	FAU_STG_EXT.1
توانایی به‌روزرسانی خود، مستقل از مدیر بسته یا دیگر قابلیت‌های ارائه‌شده توسط سکو زیرین.	FMT_MOF.1(1)
	FPT_TUD_EXT.1/به‌روزرسانی امن
توانایی استفاده از پیمانه‌های رمزنگاری درونی خود برای برقراری یک ارتباط امن پروتکل اینترنتی (IPsec) با NAS	FCS_IPSEC_EXT.1
مسئولیت انبارش اعتبارنامه‌های اجرایی مستقل از (علاوه بر) محافظت‌های ارائه شده توسط سکو زیرین.	FPT_APW_EXT.1
مسئولیت انبارش داده‌های امنیتی رمزنگاری مستقل از (علاوه بر) محافظت‌های ارائه شده توسط سکو زیرین.	FPT_SKP_EXT.1

۵-۴-۳- ممیزی امنیتی

شماره الزام	نام الزام
۲۶	**تولید داده ممیزی ۱**
محصول باید قادر به تولید رکوردهای ممیزی از رویدادهای قابل ممیزی زیر باشد: ۱. آغاز و پایان توابع ممیزی ۲. تمام رویدادهای قابل ممیزی برای سطوح [مشخص نشده] ممیزی؛ و ۳. تمام فعالیت‌های اجرایی متشکل از: a. تنظیم و پیکربندی راز مشترک RADIUS b. تغییرات پیکربندی مرتبط با ارتباط با NAS یا دیگر مؤلفه‌های مستقر در محیط عملیاتی c. پیکربندی رمزنگاری یا تنظیمات مرتبط با امنیت d. پیکربندی خط‌مشی‌ها، طرح‌ها یا فاکتورهای دیگری که نحوه اعمال احراز هویت کاربر توسط محصول را کنترل می‌کنند. رویدادهای قابل ممیزی که به‌صورت خاص تعریف‌شده و در جدول ۶ (رویدادهای قابل ممیزی) آورده شده‌اند.	
۲۷	**تولید داده ممیزی ۲**
محصول باید با هر رکورد ممیزی حداقل اطلاعات زیر را ثبت کند: ۱. تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و خروجی رویداد (موفقیت یا شکست)؛ ۲. برای هر نوع رویداد قابل ممیزی، بر اساس تعاریف رویداد قابل ممیزی مؤلفه‌های کارکردی موجود در هدف امنیتی یا بسته الحاقی، اطلاعات مشخص شده در ستون سوم جدول ۶ (رویدادهای قابل ممیزی). **نکته کاربردی ۱۴:** جدول زیر رویدادهای قابل ممیزی را برای الزامات کارکرد امنیتی تعریف می‌کند که توسط بسته الحاقی در بخش ۵-۲ اجباری شده‌اند و همچنین آن الزاماتی که برای کاربرد محصول در بخش ۵-۴ اجباری شده‌اند. اگر محصول ادعایی به‌غیراز این الزامات کارکرد امنیتی داشته باشد، نویسنده هدف امنیتی باید تمام	

رویدادهای قابل ممیزی مرتبط با این الزامات کارکرد امنیتی که از جانب منبع مناسب ادعا شده‌اند را به این جدول اضافه کند، برای مثال هر الزامات کارکرد امنیتی اختیاری که از پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) گرفته شده است و مانند بخش ۵-۴-۲ باید شامل رویدادهای قابل ممیزی مرتبط تعریف شده در آن پروفایل حفاظتی باشد.

جدول ۵ رویدادهای قابل ممیزی

الزام	رویدادهای قابل ممیزی	محتویات رکورد ممیزی اضافی
FCO_NRO.1	سرویس گیرنده درخواست چیزی را می‌کند که محصول راز مشترکی با آن ندارد	هویت کاربر، محتویات پاسخ EAP (در صورت وجود)
FCO_NRR.1	هیچ	هیچ
FCS_EAP-TLS_EXT.1	شکست پروتکل، برقراری نشست TLS	اگر شکست اتفاق بیفتد، دلیلی توصیفی برای آن ثبت شود.
FCS_RADIUS_EXT.1	شکست پروتکل موفقیت یا شکست احراز هویت	اگر شکست اتفاق بیفتد، دلیلی توصیفی برای آن ثبت شود.
FCS_RADSEC_EXT.1 (مبتنی بر انتخاب)	شکست در برقراری نشست RadSec	دلایلی برای شکست
FIA_PSK_EXT.1	هیچ‌کدام	هیچ‌کدام
FIA_UAU.6 (اختیاری)	تمام استفاده‌های سازوکار احراز هویت	مبدأ تلاش (برای مثال آدرس پروتکل اینترنتی (IP))

الزام	رویدادهای قابل ممیزی	محتویات رکورد ممیزی اضافی
FMT_SMR.2	أ. تغییرات برای گروهی از کاربران که قسمتی از یک نقش هستند. ب. تلاش‌های ناموفق برای استفاده از نقش به دلیل شرایط داده شده به نقش	شناسه کاربرانی که با تغییرات مرتبط هستند هویت مدیر سیستمی که توابع را اجرا می‌کند.
FPT_TST_EXT.1	اجرای مجموعه‌ای از خودآزمایی‌های پیمانه رمزنگاری	هیچ اطلاعات اضافی دیگری
FTA_TSE.1	انکار برقراری نشست به‌واسطه سازوکار برقراری نشست	دلایل انکار، مبدأ تلاش برای برقراری
FTP_ITC.1	راه‌اندازی (آغاز) کانال امن به پایان رساندن کانال امن شکست در توابع کانال امن	شناسایی آغازکننده ارتباط و هدف از تلاش‌های شکست‌خورده برای برقراری کانال امن

۵-۴-۴- مدیریت امنیت

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

نکته کاربردی ۱۵: الزامات کارکرد امنیتی اضافه‌ای برای مدیریت امنیت وجود ندارد. با این وجود، کارکردهای مدیریتی دیگری نیز هستند که برای توسعه الزام کارکرد امنیتی - مشخصات کارکرد مدیریتی (FMT_SMF.1) مربوط به الزامات کارکرد امنیتی موجود در پروفایل حفاظتی برنامه کاربردی (App PP) به کار می‌روند. به همین ترتیب، رویدادهای زیر برای انطباق اهداف امنیتی باید با رویدادهای پروفایل حفاظتی برنامه کاربردی (App PP) ترکیب شوند.

- توانایی برای تنظیم راز به اشتراک گذاشته شده RADIUS
- توانایی برای تعریف NAS مجاز
- توانایی برای فعال کردن، غیرفعال کردن، تعیین و تغییر رفتار تمام محصول که در این بسته الحاقی برای مدیر سیستم شناسایی شده‌اند.
- [انتخاب: توانایی برای تنظیم و پیکربندی کارکرد IPsec،

هیچ تابع دیگری]	
۲۹	**محدودیت‌هایی بر روی نقش‌های امنیتی ۱**
محصول باید نقش‌های زیر را حفظ کنند: **– مدیر سیستم**	
۳۰	**محدودیت‌هایی بر روی نقش‌های امنیتی ۲**
محصول باید بتواند کاربران را به نقش‌ها ارتباط دهند.	
۳۱	**محدودیت‌هایی بر روی نقش‌های امنیتی ۳**
محصول باید از برآورده شدن شروط زیر اطمینان حاصل کند: – نقش مدیر سیستم باید قادر به اجرای محصول به‌صورت محلی باشد. – نقش مدیر سیستم باید قادر به اجرای محصول به‌صورت راه دور باشد	

۵-۴-۵- محافظت از محصول

شماره الزام	نام الزام
۳۲	**آزمون محصول توسعه‌یافته ۱**
محصول باید مجموعه‌ای از خودآزمایی‌های زیر را اجرا کند [انتخاب: در طول راه‌اندازی اولیه (با روشن کردن)، به‌صورت دوره‌ای در حین فعالیت عادی، هنگام درخواست یک کاربر مجاز، تحت شرایطی [اختصاص: *شرایطی که تحت آن خودآزمایی باید رخ دهد*] تا نشان‌دهنده عملکرد صحیح محصول باشد: [اختصاص: *فهرستی از خودآزمایی‌هایی که توسط محصول اجرا می‌شوند*] است].	

۶- الزامات تضمین امنیت

این بسته الحاقی هیچ الزامات تضمین امنیتی دیگری به‌جز آن‌هایی را که در پروفایل حفاظتی مبنا تعریف‌شده و ادعای انطباق با آن داشته، تعریف نکرده است. باید توجه شود محصولی که بر اساس این بسته الحاقی ارزیابی می‌شود به‌طور طبیعی در مقابل پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) و یا پروفایل حفاظتی برنامه کاربردی (App PP) نیز ارزیابی خواهد شد. پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) و پروفایل حفاظتی برنامه کاربردی (App PP) هر دو اقدامات تضمینی را شامل می‌شوند که با الزامات کارکرد امنیتی (SFR) و الزامات تضمین امنیتی (SAR) مرتبط هستند. علاوه بر این، در این بسته الحاقی تعدادی از اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی آورده شده‌اند که به‌طور مشابه الزامات تضمین امنیتی پروفایل حفاظتی مبنا را اصلاح می‌کند. آزمایشگاه ارزیابی محصول را بر اساس پروفایل حفاظتی مبنا ارزیابی می‌کند و ارزیابی با الزامات کارکرد امنیتی ضروری که توسط این بسته الحاقی اتخاذ شده‌اند را پیوست می‌کند.

۶-۱- اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی

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

۶-۱-۱- اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی بسته الحاقی

جدول ۶ اقدامات تضمین الزام اثبات مبدأ انتخابی

اقدامات تضمینی الزام کارکرد امنیتی ارتباطات - اثبات مبدأ انتخابی	
خلاصه مشخصه محصول[۳۳] (TSS)	ارزیاب باید شرح پیاده‌سازی این پروتکل را بررسی نماید تا اطمینان حاصل شود که احرازهویت‌کنندگان پیام EAP کپسوله‌شده[۳۴] RADIUS مطابق با RFC 3579 است.
سند راهنمای اجرایی[۳۵] (AGD)	ارزیاب باید بررسی کند که راهنماها در بردارنده دستورالعمل‌های لازم برای پیکربندی RADIUS و EAP کپسوله‌شده بر روی محصول است تا اطمینان حاصل کند که شواهدی از مبدأ برای تمام بسته‌های RADIUS Access-Request جمع‌آوری و نگهداری می‌شوند.
آزمون (Test)	ارزیاب باید آزمون‌های زیر را انجام دهد: آزمون ۱: ارزیاب باید یک RADIUS Access-Request را از یک NAS که محصول راز RADIUS را با آن به اشتراک نگذاشته است، با خصیصه‌های شناسایی NAS که به‌درستی نشان‌دهنده مبدأ سرور دسترسی شبکه (NAS) بوده و دربرگیرنده یک پیام پاسخ EAP کپسوله‌شده و خصیصه معتبر احراز هویت کننده پیام است ارسال کند. ارزیاب باید تائید کند که محصول پیام را بدون پاسخ رها می‌کند. آزمون ۲: ارزیاب باید یک RADIUS Access-Request را از یک NAS که محصول راز RADIUS را با آن به اشتراک نگذاشته است، با خصیصه‌های شناسایی NAS که به اشتباه نشان‌دهنده یک سرور دسترسی شبکه (NAS) بوده که محصول راز RADIUS را با آن به اشتراک گذاشته است و دربرگیرنده یک پیام پاسخ EAP کپسوله‌شده و خصیصه معتبر احراز هویت کننده پیام است ارسال کند. ارزیاب باید تائید کند که محصول پیام را بدون پاسخ رها می‌کند.

[۳۳] TOE Summary Specification

[۳۴] encapsulated

[۳۵] Administrative guidance document

جدول ۷ اقدامات تضمین الزام اثبات دریافت انتخابی

اقدامات تضمینی الزام کارکرد امنیتی ارتباطات - اثبات دریافت انتخابی	
خلاصه مشخصه محصول (TSS)	ارزیاب باید شرح پیاده‌سازی این پروتکل را بررسی کند تا اطمینان حاصل کند که احراز هویت کننده پاسخ RADIUS مطابق با RFC 2865 است.
سند راهنمای اجرایی (AGD)	ارزیاب باید بررسی کند که راهنماها دربرگیرنده دستورالعمل‌های لازم برای پیکربندی RADIUS و EAP کپسوله‌شده بر روی محصول است تا اطمینان حاصل کند که شواهدی از اعلام وصول برای تمام بسته‌های RADIUS Access-Request واردشده، ایجاد شده و به‌درستی انتقال می‌یابند.
آزمون (Test)	ارزیاب باید آزمون زیر را انجام دهد: آزمون ۱: ارزیاب باید یک RADIUS Access-Request شامل پیام پاسخ EAP کپسوله‌شده از نوع هویت، تعیین یک حساب کاربری معتبر، خدماتی که کاربر را مجاز می‌کند و شامل همه اطلاعات مورد نیاز برای احراز هویت کاربر باشد. ارزیاب باید بررسی کند که محصول پیام Access-Challenge[۳۶] برمی‌گرداند و چکیده پیام[۳۷] الگوریتم خلاصه پیام[۳۸] (MD5 Hash) از کد متن طولانی+ شناسه + طول + احراز هویت کننده درخواست Access-Request + خصیصه‌ها + راز با پاسخ احراز هویت کننده مطابقت دارد.

جدول ۸: اقدامات تضمین الزام امنیت لایه انتقال توسعه‌یافته

[۳۶] Access-Challenge

[۳۷] hash

[۳۸] message-digest algorithm

اقدامات تضمینی الزام کارکرد امنیتی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر – امنیت لایه انتقال (EAP-TLS) توسعه‌یافته	
خلاصه مشخصه محصول (TSS)	ارزیاب باید شرح پیاده‌سازی این پروتکل را در خلاصه مشخصه محصول بررسی کند تا اطمینان حاصل نماید که مشخصات اختیاری (مثل الحاقیه‌های پشتیبانی شده) و دنباله رمزهای پشتیبانی شده مشخص شده‌اند. ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا از یکسانی دنباله رمزهای مشخص‌شده با آن‌هایی که برای این مؤلفه ذکر شده‌اند اطمینان حاصل کند.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنمای عملیاتی را بررسی کند تا اطمینان یابد که دستورالعمل‌هایی برای مدیران سیستم وجود دارد تا فهرستی از مراجع صلاحیت‌دار صدور گواهی را که مجوز امضای گواهی‌ها با استفاده از سرور احراز هویتی که در تبادلات احراز هویت توسعه‌پذیر – امنیت لایه انتقال (EAP-TLS)، مورد پذیرش محصول هستند، مشخص نماید و نیز دستورالعمل‌هایی در مورد نحوه تعیین مجموعه الگوریتم‌های پیشنهاد شده و پذیرفته‌شده توسط محصول در طول تبادلات EAP-TLS دارد. همچنین ارزیاب باید راهنمای عملیاتی را برای اطمینان از داشتن دستورالعمل‌هایی در مورد پیکربندی محصول بررسی کند به‌طوری‌که امنیت لایه انتقال (TLS) با توضیحات خلاصه مشخصه محصول مطابقت داشته باشد (برای مثال مجموعه دنباله رمزهای انتشار داده شده توسط محصول ممکن است برای برآوردن این الزامات محدود شود).
آزمون (Test)	ارزیاب باید آزمون‌های زیر را انجام دهد: آزمون ۱: ارزیاب باید ارتباط TLS را با استفاده از هر دنباله رمز مشخص‌شده در این الزام برقرار کند. این ارتباط ممکن است به‌عنوان قسمتی از برقراری پروتکل سطح بالاتر مثلاً قسمتی از نشست EAP برقرار شود. مشاهده مراوده موفقیت‌آمیز یک دنباله رمز (روی سیم) برای برآوردن هدف آزمون کافی است؛ بررسی مشخصه‌های ترافیک رمزگذاری شده در تلاش جهت تشخیص اینکه دنباله رمزی که مورد استفاده قرار گرفته است ضروری نیست (برای مثال، تشخیص اینکه الگوریتم رمزنگاری مورد استفاده استاندارد رمزگذاری پیشرفته (AES) ۱۲۸ بیتی بوده و استاندارد رمزگذاری پیشرفته (AES) ۲۵۶ بیتی نیست). آزمون ۲: آزمون‌های زیر برای هر گواهی پشتیبانی شده با امضای الگوریتم پشتیبانی شده تکرار می‌شود. ارزیاب باید برای برقراری ارتباطاتی تلاش کند که در آن گواهی سرویس گیرنده شامل هدف احراز هویت سرویس گیرنده در فیلد KeyUsage توسعه‌یافته بوده و بیت توافق کلید در فیلد KeyUsage توسعه‌یافته

	تنظیم شده و تأیید کند که ارتباط برقرارشده است. ارزیاب بعد از آن بررسی خواهد کرد که آن ارتباط با گواهی سرویس گیرنده معتبر دیگری که فاقد هدف احراز هویت سرویس گیرنده در فیلد KeyUsage توسعه‌یافته است برقرار نشده است. آزمون ۳: ارزیاب باید برای تنظیم فهرستی از پروتکل‌هایی که باید در طول مبادلات EAP-TLS پیشنهاد شود راهنماهای اجرایی را دنبال کند، این پروتکل‌ها باید تنها به مواردی محدود باشند که توسط عنصر اول این مؤلفه مشخص شده است. ارزیاب باید ارتباطی با یک NAS آغاز کرده و اطمینان حاصل نماید که فقط پروتکل‌های پیکربندی‌شده پیشنهاد داده می‌شوند. اگر فهرست اولیه زیرمجموعه‌ای از مجموعه کلی پروتکل‌های پیشنهادشده توسط سرویس گیرنده نباشد، ارزیاب باید آزمون را تکرار کند تا زیرمجموعه‌ای از پروتکل‌های مورداستفاده در آزمون آغازین مشخص شود.

جدول ۹: اقدامات تضمین الزام RADIUSتوسعه‌یافته

اقدامات تضمین الزام کارکرد امنیتی پشتیبانی رمزنگاری RADIUS توسعه‌یافته	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را به‌منظور حصول اطمینان از اینکه RADIUS به‌عنوان پروتکلی تعیین‌شده است که همه ارتباطات میان محصول و سرور دسترسی شبکه (NAS) بر اساس آن انجام می‌شود، بررسی کند. ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا اطمینان حاصل کند که EAP به‌عنوان یک پروتکل احراز هویت مورد استفاده برای ارتباط میان محصول و NAS مشخص شده است و امنیت لایه انتقال (TLS) ابزاری برای احراز هویت دوطرفه‌ای است که باید بر روی EAP انجام شود و دیگر چارچوب‌های احراز هویت غیرمجاز هستند. ارزیاب باید توضیحات مربوط به پیاده‌سازی این پروتکل را بررسی کند تا اطمینان حاصل شود که احراز هویت کنندگان پیام EAP کپسوله‌شده RADIUS با RFC 3579 مطابقت می‌کند.
سند راهنمای اجرایی (AGD)	ارزیاب باید تأیید کند که راهنما، دستورالعمل‌های ضروری برای پیکربندی RADIUS و EAP-TLS کپسوله‌شده بر روی محصول مطابق با RFCهای ۲۸۶۵، ۲۸۶۹، ۳۵۷۹ و ۵۲۱۶ در برمی‌گیرد.
آزمون (Test)	ارزیاب باید آزمون‌های زیر را انجام دهد: آزمون ۱: ارزیاب باید درخواست دسترسی RADIUS را با پیام‌های پاسخ EAP کپسوله‌شده برای محصول، از یک NAS با محصول که یک کلید از قبل به اشتراک گذاشته‌شده RADIUS را به اشتراک می‌گذارد ارسال کرده و تائید کند که محصول مطابق با RFCهای ۲۸۶۵ و ۳۵۷۹ به‌درستی به این پیام‌ها پاسخ می‌دهد.

	• یک Access-Request شامل یک پیام پاسخ EAP کپسوله‌شده است. ارزیاب باید تائید کند که محصول یک Access-Reject شامل پاسخ EAP کپسوله‌شده از نوع تصدیق منفی[۳۹] (NaK) را برمی‌گرداند که نشان‌دهنده عدم جایگزین است. • یک Access-Request شامل پیام‌های پاسخ EAP کپسوله‌شده و هر یک از خصیصه‌های[۴۰] زیر است: User-password, CHAP[۴۱]-password, CHAP-challenge, ARAP-password, password-retry, reply-message, error-cause. ارزیاب باید بررسی کند که در هر مورد محصول درخواست‌ها را بدون پاسخ رها می‌کند. • یک Access-Request که شامل یک پیام پاسخ EAP کپسوله‌شده بوده و هیچ خصیصه احراز هویت کننده پیامی را در برنمی‌گیرد. ارزیاب باید تأیید کند که محصول درخواست را بدون پاسخ رها می‌کند. • یک Access-Request شامل یک پیام پاسخ EAP کپسوله‌شده از نوع MD5-challenge است. ارزیاب باید تأیید کند که محصول با پیام Access-Challenge از نوع تصدیق منفی (NaK) یا تصدیق منفی (NaK) توسعه‌یافته به این پیام پاسخ می‌دهد. • یک Access-Request شامل یک پیام پاسخ EAP کپسوله‌شده از نوع هویت است که مشخص‌کننده یک حساب کاربری معتبر و خدمتی است که کاربر برای آن مجاز شده و شامل همه اطلاعات مورد نیاز برای احراز هویت کاربر است. ○ ارزیاب باید تائید کند که محصول یک Access-Challenge را با یک بسته شروع پروتکل EAP-TLS کپسوله‌شده برمی‌گرداند؛ مانند: EAP-request با تنظیم EAP-type به EAP-TLS، تنظیم بیت شروع و no data. ○ ارزیاب باید به تکمیل دست‌دهی TLS با ارائه گواهی‌نامه‌های سرویس گیرنده معتبر، غیرامن، منقضی شده و لغو شده برای محصول ادامه دهد و تأیید کند که پیام دست دهی تنها برای گواهی‌نامه‌های معتبر با موفقیت به اتمام می‌رسد و برای بقیه ناموفق ست. ○ ارزیاب باید تأیید کند که محصول یک دست‌دهی TLS موفقیت‌آمیز را با access-accept همراه با بسته EAP-success کپسوله‌شده نشان می‌دهد. ارزیاب باید تائید کند که محصول یک دست دهی TLS ناموفق را با Access-

[۳۹] Negative-Acknowledgement

[۴۰] attributes

[۴۱] Challenge Handshake Authentication Protocol

	Reject همراه با بسته EAP-failure کپسوله‌شده نشان می‌دهد. ○ در طول دیگر دست‌دهی‌های موفق، ارزیاب باید Access-Request با EAP-response کپسوله‌شده با EAP-type تنظیم‌شده را به هر چیزی به‌جز EAP-TLS ارسال کند و بررسی کند که محصول یک Access-challenge با EAP-Reques کپسوله‌شده از نوع EAP-TLS برمی‌گرداند که نشان‌دهنده error-cause است: خطای نوع EAP نامعتبر (نادیده گرفته شده). ارزیاب باید تائید کند که مراحل متوالی دست دهی به‌صورت عادی کامل می‌شوند. • در طول دیگر دست‌دهی‌های موفق، ارزیاب باید پنج Access-Request را با بسته‌های EAP نامعتبر کپسوله‌شده ارسال کند و تائید کند که محصول بعد از دریافت پنجمین بسته نامعتبر، Access-Reject را با بسته EAP-failure کپسوله‌شده ارسال می‌کند. • یک Access-Request شامل پیام EAP-response کپسوله‌شده از نوع شناسه است که یک حساب کاربری معتبر و خدماتی که کاربر برای آن‌ها مجاز نیست را مشخص می‌کند. ارزیاب باید تائید کند که محصول Access-Reject را برمی‌گرداند. • یک Access-Request شامل پیام EAP-response کپسوله‌شده از نوع شناسه است که یک حساب کاربری نامعتبر را مشخص می‌کند. ارزیاب باید تائید کند که محصول Access-Reject را برمی‌گرداند. • یک Access-Request که رشته طول آن نادرست است. ارزیاب باید تائید کند که محصول درخواست را بدون پاسخ رها می‌کند. • یک Access-Request که رشته کد آن نامعتبر است. ارزیاب باید تائید کند که محصول درخواست را بدون پاسخ رها می‌کند. • یک Access-Request که یک پیام EAP- response کپسوله‌شده و خصیصه احراز هویت کننده پیام را در برمی‌گیرد که با درخواست مطابقت ندارد. ارزیاب باید تائید کند که محصول درخواست را بدون پاسخ رها می‌کند.

جدول ۱۰: اقدامات تضمین الزام ترکیب کلید از قبل به اشتراک‌گذاری شده

اقدامات تضمین الزام کارکرد امنیتی شناسایی و احراز هویت ترکیب کلید از قبل به اشتراک گذاشته شده

خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا مطمئن شود که خلاصه مشخصه محصول تمام پروتکل‌هایی را که اجازه کلید از قبل به اشتراک گذاشته شده متنی را دارند شناسایی می‌کند و توضیح می‌دهد که کلیدهای از قبل به اشتراک گذاشته شده متنی دارای ۲۲ کاراکتر برای هر پروتکل شناسایی‌شده توسط این الزام پشتیبانی می‌شوند. ارزیاب همچنین باید تأیید کند که انتخاب IPsec یا امنیت خدمت RadSec با انتخاب الزام کارکرد امنیتی مسیر امن – کانال امن درونی محصول (FTP_ITC.1) مطابقت دارد.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنمایی عملیاتی را بررسی کند تا تعیین کند که راهنمایی‌هایی در مورد ترکیب کلیدهای از قبل به اشتراک گذاشته متنی قوی را برای مدیران سیستم ارائه می‌دهد (و اگر انتخاب کلیدهایی با طول‌های متنوع را نشان می‌دهد که می‌توان وارد کرد)، اطلاعاتی در مورد گستره طول‌های پشتیبانی شده ارائه می‌دهد. راهنمایی‌ها باید کاراکترهای مجاز برای کلیدهای از قبل به اشتراک گذاشته را مشخص کند و این فهرست باید مجموعه مرجعی از دیگر مجموعه فهرست‌های موجود در الزام کارکرد امنیتی شناسایی و احراز هویت ترکیب کلید از قبل به اشتراک گذاشته شده توسعه‌یافته.۱,۲ (FIA_PSK_EXT.1.2) باشد.
آزمون (Test)	ارزیاب باید آزمون‌های زیر را بر روی هرکدام از پروتکل‌ها (نصب یک پروتکل درصورتی‌که توسط پیاده‌سازی‌های متفاوت محصول انجام شده باشد) انجام دهد. توجه داشته باشید که بر روی هر گزینه آزمون می‌توان یک یا چندین آزمون را انجام داد. آزمون ۱: ارزیاب باید یک کلید از قبل به اشتراک گذاشته شده ۲۲ کاراکترای را تشکیل دهد که شامل ترکیبی از کاراکترهای مجاز مطابق با راهنمای عملیاتی است و نشان دهد که مراوده پروتکلی موفق می‌تواند با این کلید انجام شود. آزمون ۲ [شرطی]: اگر محصول از کلیدهای از قبل به اشتراک گذاشته شده با طول‌های متفاوت پشتیبانی کند، ارزیاب باید آزمون یک را برای کمترین طول، بیشترین طول، طولی در گستره مجاز و طول‌های نامعتبر خارج از گستره پشتیبانی شده (هم حد بالا و هم حد پایین) تکرار کند. آزمون‌های مربوط به بیشترین طول، کمترین طول و طول در گستره مجاز باید موفقیت‌آمیز باشند و طول‌های نامعتبر باید توسط محصول رد شوند.

جدول ۱۱: اقدامات تضمین الزام برقراری نشست محصول

اقدامات تضمین پالایش الزام کارکرد امنیتی دسترسی به محصول – برقراری نشست محصول

خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا تمام خصیصه‌هایی که ممکن است با توجه به آن‌ها نشست کاربر انکار شود، به شکل مشخصی تعریف شده باشد.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنمای عملیاتی را بررسی کند تا تعیین کند که این راهنما دربرگیرنده راهنمایی‌هایی در مورد پیکربندی هر یک از خصیصه‌های شناسایی‌شده در خلاصه مشخصه محصول است.
آزمون (Test)	ارزیاب باید آزمون زیر را برای هرکدام از خصیصه‌ها انجام دهد: آزمون ۱: ارزیاب باید یک نشست کاربر را با موفقیت برقرار کند. ارزیاب باید از راهنمای عملیاتی برای پیکربندی سامانه تبعیت کند به‌گونه‌ای که دسترسی آن کاربر بر اساس یک مقدار خاص از خصیصه انکار شود. پس‌ازآن ارزیاب برای برقراری یک نشست در تضاد با تنظیمات خصیصه تلاش می‌کند در حالی که هنوز داده احراز هویت معتبر ارائه می‌دهد. ارزیاب باید مشاهده کند که تلاش برای دسترسی با شکست مواجه شده است. ارزیاب باید این آزمون را برای هر خصیصه مشخص شده توسط نویسنده هدف امنیت تکرار کند.

جدول ۱۲: اقدامات تضمین الزام کانال امن درونی محصول

اقدامات تضمین الزام کارکرد امنیتی مسیر/کانال امن - کانال امن درونی محصول	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا تعیین کند که برای تمام ارتباطات با موجودیت‌های فناوری اطلاعات مجاز شناسایی‌شده در الزام، هر سازوکار ارتباطی از دیدگاه پروتکل‌های مجاز برای آن موجودیت فناوری اطلاعات شناسایی‌شده است. ارزیاب همچنین باید تأیید کند که همه پروتکل‌های ذکرشده در خلاصه مشخصه محصول شناسایی‌شده و در الزامات هدف امنیتی گنجانده شده‌اند.
سند راهنمای اجرایی (AGD)	ارزیاب باید تأیید کند که مستندات راهنما دستورالعمل‌هایی برای ایجاد و برقراری مجدد تمام پروتکل‌های مجاز با هر موجودیت فناوری اطلاعات مجاز را در برمی‌گیرد.
آزمون (Test)	ارزیاب باید آزمون زیر را انجام دهد: آزمون ۱: ارزیاب باید مطمئن شود که ارتباطات با هر NAS با استفاده از هر پروتکل در طول دوره ارزیابی آزموده شده است و ارتباطات با توجه به اسناد

	راهنما تنظیم شده‌اند و باید اطمینان حاصل کند که ارتباطات موفقیت‌آمیز بوده‌اند. آزمون ۲: برای هر پروتکل که محصول می‌تواند با توجه به آنچه در الزام آمده است آغاز کند، ارزیاب باید از اسناد راهنما پیروی کند تا مطمئن شود که در عمل کانال ارتباطی می‌تواند با موفقیت از محصول آغاز گردد. آزمون ۳: ارزیاب باید در مورد هر کانال ارتباطی با NAS مطمئن شود که کانال داده از پروتکل‌های شناسایی‌شده مناسبی استفاده می‌کند. آزمون ۴: ارزیاب باید برای هر پروتکل مرتبط با NAS که با آزمون ۱ مورد آزمایش قرار گرفته‌اند به‌صورت فیزیکی تداخلی در یک ارتباط برقرارشده ایجاد کند. ارزیاب باید مطمئن شود که وقتی ارتباط فیزیکی دوباره وصل شد ارتباطات دوباره به‌صورت مناسبی محافظت می‌شوند. فعالیت‌های تضمینی بیشتر که با پروتکل‌های خاص مرتبط هستند در الزام کارکرد امنیتی مسیر/ کانال امن - کانال امن درونی محصول (FTP_ITC.1.1) قابل انتخاب هستند.

۶-۱-۲- اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی پروفایل حفاظتی مشترک افزاره شبکه (NDcPP)

جدول ۱۳: اقدامات تضمین الزام تولید داده امنیتی

اقدامات تضمین الزام کارکرد امنیتی ممیزی امنیتی - تولید داده ممیزی
ارزیاب باید اقدام تضمینی برای الزامات کارکرد امنیتی ممیزی امنیتی - تولید داده ممیزی (FAU_GEN.1) را علاوه بر رویدادهای قابل ممیزی کاربردپذیر تعریف‌شده در پروفایل حفاظتی مشارکتی افزاره شبکه، به همان شکلی که در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) برای رویدادهای قابل ممیزی بالا تعریف شده است انجام دهد. علاوه بر این ارزیاب باید تضمین کند که فعالیت‌های اجرایی تعریف شده برای این بسته الحاقی به‌طور مناسبی ممیزی شده‌اند.

جدول ۱۴: اقدامات تضمین الزام ساماندهی شکست احراز هویت

اقدامات تضمین الزام کارکرد امنیتی شناسایی و احراز هویت - ساماندهی شکست احراز هویت	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را برای داشتن توصیفی برای هر روش پشتیبانی شده برای اقدامات اجرایی از راه دور بررسی کند تا مشخص کند که چگونه تلاش‌های احراز هویت ناموفق پی‌درپی شناسایی و ردیابی می‌شود. خلاصه مشخصه محصول همچنین باید روشی را شرح دهد که با استفاده از آن مانع از ورود موفق مدیر سیستم از راه دور به محصول شده و اقدامات ضروری برای حفظ این توانایی را شرح دهد.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنمای عملیاتی را بررسی کند تا مطمئن شود دستورالعملی برای تنظیم حد آستانه شکست احراز هویت و نحوه پاسخ محصول هنگام رسیدن به این حد آستانه تعریف شده باشد (چنانچه قابل تنظیم باشد) و فرآیندی برای هر «اقدام» مشخص شده شرح داده شده است که به مدیر راه دور اجازه می‌دهد تا یک‌بار بتواند به سیستم وارد شود (درصورتی‌که این گزینه انتخاب شود). اگر اقدام یا سازوکار متفاوت دیگری با توجه به مسیر امن مورد استفاده برای دسترسی محصول پیاده‌سازی شده باشد تمام آن‌ها با جزییات توضیح داده شود (الزام کارکرد امنیتی مسیر/کانال امن – مسیر امن (FTP_TRP.1) را ببینید).
آزمون (Test)	ارزیاب باید آزمون‌های زیر را برای هر روشی که از طریق آن مدیر سیستم راه دور به محصول دسترسی دارد انجام دهد: آزمون ۱: ارزیاب باید از راهنماهای عملیاتی برای تنظیم تعداد تلاش‌های احراز هویت ناموفق پی‌درپی مجاز توسط محصول استفاده کند. ارزیاب باید زمانی که به حد آستانه برای حساب مدیر سیستم از راه دور رسیده باشد، آزمون را انجام داده و مطمئن شود که تلاش‌های بعدی حتی با اعتبارنامه‌های معتبر موفقیت‌آمیز نخواهند بود. آزمون ۲: [شرطی] اگر خلاصه مشخصه محصول نشان دهد که برای فعال‌سازی مجدد حساب کاربری که به دلیل شکست‌های احراز هویت بیش از حد مسدود شده، یک اقدام مدیریتی ضروری است، ارزیاب باید برای قفل‌کردن یک حساب کاربری مراحل موجود در آزمون ۱ را انجام دهد، از راهنمای عملیاتی برای فعال‌سازی مجدد حساب مدیریتی قفل‌شده به‌صورت دستی پیروی کرده و مشاهده کند که یک‌بار دیگر قادر به ورود موفقیت‌آمیز مدیر سیستم است. آزمون ۳: [شرطی] اگر خلاصه مشخصه محصول نشان دهد که یک بازه زمانی باید سپری شود تا یک حساب کاربری که به دلیل شکست‌های احراز هویت بیش از حد مسدود شده مجدداً به‌صورت خودکار فعال شود، ارزیاب باید مراحل موجود در آزمون ۱ را انجام دهد تا یک حساب را قفل کند، از راهنمای عملیاتی برای تنظیم بازه‌های زمانی قابل انتخاب پیروی کند و مشاهده کند در طول تلاش‌های ورود دوره‌ای، حساب کاربری نمی‌تواند به‌صورت موفقیت‌آمیز

	وارد شود تا مقدار زمانی تنظیم شده سپری شود. ارزیاب باید این آزمون را برای بازه‌های زمانی متفاوت قابل انتخاب آزمایش کند.

جدول ۱۵: اقدامات تضمین الزام مشخصات توابع مدیریت

اقدامات تضمین الزام کارکرد امنیتی مدیریت امنیت - مشخصات توابع مدیریت
انطباق با دیگر الزامات کارکرد امنیتی در بخش ۵-۲ و ۵-۳ این بسته الحاقی و هر الزام کارکرد امنیتی کاربردپذیر در پیوست‌ها برای نشان دادن این موضوع که محصول ابزارهای کافی برای مدیریت توابع سرور احراز هویت خویش فراهم آورده است، کافی است.

۶-۱-۳-اقدامات تضمین مبتنی بر الزامات کارکرد امنیتی پروفایل حفاظتی برنامه کاربردی (App PP)

جدول ۱۶: اقدامات تضمین الزام تولید داده ممیزی

اقدامات تضمین الزام کارکرد امنیتی ممیزی امنیت - تولید داده ممیزی	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند و مطمئن شود که قالب مناسب برای رکوردهای ممیزی را فراهم می‌کند. در کنار شرح مختصری برای هر رشته، هر قالب ثبت ممیزی باید پوشش داده شوند.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنمای عملیاتی را بررسی کند و مطمئن شود که فهرستی از تمام رویدادهای قابل‌بررسی را در خود دارد و قالبی برای همه رکوردهای ممیزی فراهم می‌آورد. هر نوع قالب رکورد ممیزی باید پوشش داده‌شده و خلاصه مختصری برای هر رشته ارائه شود. ارزیاب باید مطمئن شود که تمامی انواع رویدادهای قابل ممیزی برای بسته الحاقی اجبار شده‌اند و شرح رشته‌ها دربرگیرنده اطلاعات موردنیاز الزام کارکرد امنیتی ممیزی امنیت - تولید داده ممیزی (FAU_GEN.1.2) و اطلاعات اضافی مشخص‌شده در جدول ۴ هستند. ارزیاب باید به‌صورت ویژه اطمینان یابد که راهنمای عملیاتی در رابطه با محتویات رویدادهای رشته‌ای واضح است. در جدول ۴ جزئیات اطلاعات این رویداد و یک نام یا شناسه برای منشأ رویداد مورد نیاز است. ارزیاب باید مطمئن شود که نام یا شناسه در راستای اجازه دادن به مدیر سیستم برای بازنگری ثبت‌های ممیزی به‌منظور تعیین محتوای عملیات و نقطه انتهایی غیر محصول ارتباط برای شکست‌های مرتبط با ارتباطات با دیگر سامانه‌های فناوری اطلاعات کفایت می‌کند.

	ارزیاب باید در مورد اقدامات اجرایی که به محتوای این بسته الحاقی مرتبط هستند تصمیم‌گیری کند. ممکن است محصول قابلیت کارکردی‌ای داشته باشد که به دلیل مشخص نشدن آن قابلیت کارکردی به‌عنوان یک الزام کارکردی امنیت در محتوای این بسته الحاقی، ارزیابی نشده باشد. این قابلیت کارکردی ممکن است دارای جنبه‌های اجرایی‌ای باشد که در راهنمای عملیاتی توصیف‌شده‌اند. از آنجا که این اقدامات اجرایی در یک پیکربندی ارزیابی‌شده محصول اجرا نخواهند شد، ارزیاب باید راهنمای عملیاتی را بررسی کند و تصمیم بگیرد که کدام دستورات اجرایی شامل زیر دستورها، اسکریپت‌ها[۴۲] و فایل‌های پیکربندی مرتبط با پیکربندی (شامل فعال یا غیرفعال کردن) سازوکار پیاده‌سازی شده در محصول ضروری هستند تا الزامات مشخص‌شده در بسته الحاقی که را که مجموعه‌ای «تمام اقدامات اجرایی» را شکل می‌دهند اجرا کند. ارزیاب ممکن است این عمل را به‌عنوان قسمتی از فعالیت‌های مرتبط با تضمین راهنمای مستندات راهنمای اجرایی – راهنمای کاربر عملیاتی (AGD_OPE) که الزامات را برآورده می‌سازد، اجرا کند.
آزمون (Test)	ارزیاب باید آزمون‌های زیر را انجام دهد: آزمون ۱: ارزیاب باید توانایی محصول برای تولید صحیح رکوردهای ممیزی با داشتن محصول که این رکوردهای ممیزی را مطابق اقدامات تضمین مرتبط با الزامات کارکردی این بسته الحاقی تولید می‌کند، بیازماید. آزمون ۲: ارزیاب باید آزمایش کند که هر اقدام اجرایی کاربردپذیر در محتوای این بسته الحاقی قابل ممیزی باشد. هنگام بررسی نتایج این آزمون، ارزیاب باید مطمئن شود که رکوردهای ممیزی تولیدشده در طول آزمایش با قالب مشخص‌شده در راهنمای اجرایی مطابقت دارد و رشته‌های موجود در هر رکورد ممیزی ورودی‌های مناسبی دارند. نکته: آزمایشی که در اینجا انجام شد می‌تواند همراه با آزمودن سازوکارهای امنیتی به‌طور مستقیم انجام گیرد. برای مثال، آزمایش انجام‌شده برای نشان دادن اینکه FTE_TSE.1 به‌خوبی انکار برقراری نشست را اجرا می‌کند می‌تواند برای نشان دادن این موضوع که رکوردهای ممیزی این تابع به‌درستی تولیدشده‌اند به کار رود. اگر ارزیاب بتواند آزمایش‌های دیگر را شناسایی کند که در هرکدام رویداد قابل ممیزی تولید شده‌اند نیازی به انجام آزمایش‌های جداگانه‌ای برای آزمون انحصاری قابلیت‌های کارکردی ممیزی نیست.

[۴۲] Scripts

جدول ۱۷: اقدامات تضمین مشخصات کارکرد مدیریتی

اقدامات تضمین الزام کارکرد امنیتی مدیریت امنیت - مشخصات کارکرد مدیریتی
انطباق با دیگر الزامات کارکرد امنیتی در بخش ۵-۲ و ۵-۴ این بسته الحاقی و هر الزام کارکرد امنیتی کاربردپذیر در پیوست‌ها برای نشان دادن این موضوع که محصول ابزارهای کافی برای مدیریت توابع سرور احراز هویت خویش فراهم آورده است، کافی است.

جدول ۱۸: اقدامات تضمین الزام محدودیت‌هایی بر روی نقش‌های امنیتی

اقدامات تضمین الزام کارکرد امنیتی - محدودیت‌هایی بر روی نقش‌های امنیتی	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا تأیید کند که این خلاصه، نقش مدیر سیستم و اختیارات اعطاشده به او و محدودیت‌های نقش را توضیح می‌دهد.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنماهای عملیاتی را بررسی کند تا مطمئن شود که دستورالعمل‌هایی برای مدیریت محصول به‌صورت محلی و راه دور وجود دارد که شامل هرگونه پیکربندی‌ای است که باید در مدیریت راه دور و یا سرویس‌گیرنده اعمال شوند.
آزمون (Test)	در طول دوره اقدامات آزمایشی جهت ارزیابی، ارزیاب باید تمام رابط‌های پشتیبانی شده را مورد استفاده قرار دهد، هر چند لازم نیست هر آزمایش شامل یک اقدام اجرایی با هر رابطی تکرار شود. با این حال، ارزیاب باید مطمئن شود که هر روش پشتیبانی شده مدیریت محصول که با الزامات بسته الحاقی مطابقت دارد آزمایش‌شده است؛ برای مثال اگر محصول بتواند از طریق رابط سخت‌افزاری محلی، SSH و امنیت لایه انتقال/ پروتکل امن انتقال ابرمتن[۴۳] (TLS/HTTPS) قابل مدیریت باشد، بنابراین هر سه روش مدیریتی باید در طول اقدامات آزمایشی گروه ارزیابی اعمال شوند.

جدول ۱۹: اقدامات تضمین آزمون محصول توسعه‌یافته

اقدامات تضمین الزام کارکرد امنیتی محافظت از محصول - آزمون محصول توسعه‌یافته	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا مطمئن شود که خودآزمایی‌هایی که باید هنگام راه‌اندازی توسط محصول اجرا شود را با جزئیات شرح داده است؛ این توضیحات باید مشخص کند که چه آزمون‌هایی واقعاً در حال انجام هستند (برای مثال چیزی بیشتر از اینکه گفته شود «حافظه در حال

[۴۳] Transport Layer Security / Hypertext Transfer Protocol Secure

	آزمایش است»، توضیح باید چیزی شبیه این باشد:«حافظه با نوشتن مقداری به هر یک از مکان‌های حافظه و خواندن دوباره آن برای اطمینان از یکسانی آن با چیزی که نوشته شده بود»). ارزیاب باید تضمین کند که استدلال خلاصه مشخصه محصول در مورد کفایت آزمایش برای نشان دادن کارکرد درست محصول مناسب است.
سند راهنمای اجرایی (AGD)	ارزیاب همچنین باید مطمئن شود که دستورالعمل اجرایی خطاهای احتمالی که ممکن است از چنین آزمون‌هایی حاصل شوند و اقداماتی که مدیر باید در پاسخ انجام دهد را توضیح داده است؛ این خطاهای احتمالی باید با مواردی که در خلاصه مشخصه محصول شرح داده شده‌اند مطابقت داشته باشند.
آزمون (Test)	نسخه‌های آینده این بسته الحاقی، وجود یک مجموعه حداقلی به‌وضوح تعریف شده از خودآزمایی‌ها را اجباری خواهد کرد. برای این نسخه از بسته الحاقی انتظار می‌رود حداقل آزمایش‌های زیر انجام پذیرند: أ. درستی‌سنجی یکپارچگی میان‌افزار و نرم‌افزارهای اجرایی محصول ب.درستی‌سنجی عملیات درست توابع رمزنگاری ضروری برای برآوردن هر الزام کارکردی امنیتی. اگرچه وجود انطباق رسمی اجباری نیست، خودآزمایی‌های انجام‌گرفته باید برای یک سطح اطمینان قابل مقایسه زیر، در نظر گرفته شود: أ. فصل ۴,۹,۱ استاندارد پردازش اطلاعات فدرال انتشارات[۴۴] ۲-۱۴۰(FIPS 140-2)، آزمون یکپارچگی نرم‌افزار یا میان‌افزار به‌منظور درستی‌سنجی میان‌افزار و نرم‌افزار اجرایی ب.فصل ۴,۹,۱ استاندارد پردازش اطلاعات فدرال انتشارات ۲-۱۴۰(FIPS 140-2)، آزمون الگوریتم‌های رمزنگاری برای درستی‌سنجی عملیات درست توابع رمزنگاری باید مناسب در نظر گرفته شود. به عنوان پیشنهاد دیگر، الزامات ملی هر کشور عضو توافقنامه به رسمیت شناختن معیار مشترک[۴۵] (CCRA)، برای ارزیابی امنیت توابع رمزنگاری باید در صورت مناسب بودن در نظر گرفته شود.

[۴۴] The Federal Information Processing Standard

[۴۵] Common Criteria Recognition Arrangement

	ارزیاب ممکن است تائید کند که خودآزمایی‌هایی که در بالا به آن‌ها اشاره شد یا در طول شروع به کار اولیه اجرا شده و یا اینکه توسعه‌دهندگان دلیل هرگونه انحراف (تغییر) در آن را (در صورت امکان) توجیه کرده است.

۷- منطق الزامات امنیتی

در این بسته الحاقی، تمرکز بخش‌های آغازین سند ارائه روایت‌گونه‌ای از تلاش برای افزایش قابل فهم بودن کلی تهدیدات مورد توجه سرورهای احراز هویت؛ روش‌های مورد استفاده برای کاهش این تهدیدات و میزان کاهش دست یافته با هدف‌های ارزیابی منطبق بر این پروفایل حفاظتی بود. ساختار این ارائه به شکلی نبود که بتوان آن را با روش‌های رسمی ارزیابی کرد، بنابراین، این بخش شامل روش‌هایی با ساختار جدولی است که می‌توان از آن‌ها برای ارزیابی فعالیت‌های مرتبط با این سند استفاده کرد.

۷-۱- تعریف مسئله امنیتی

۷-۱-۱- مفروضات

شرایط خاصی که در زیر ارائه شده‌اند، فرض شده که در محیط عملیاتی محصول وجود داشته باشند. این مفروضات علاوه بر مواردی هستند که در پروفایل‌های حفاظتی مبنا تعریف شده‌اند و هم واقعیت‌های عملی در توسعه الزامات امنیتی محصول و هم شرایط محیطی ضروری در استفاده از محصول را شامل می‌شود.

جدول ۲۰-مفروضات محصول

نام فرض	تعریف فرض
A.NAS	فرض شده است محصول به سرور دسترسی شبکه (NAS) که در محیط عملیاتی قرار دارد وصل شده است که درخواست‌های احراز هویت را به آن منتقل می‌کند.

۷-۱-۲- تهدیدات

تهدیداتی که در ادامه آورده شده‌اند توسط سرور احراز هویت مورد توجه قرار دارند. توجه کنید که این تهدیدات علاوه بر مواردی هستند که در پروفایل‌های حفاظتی مبنا قرار دارند و در سرور احراز هویت اعمال شده‌اند. به‌عبارت‌دیگر، سرور احراز هویت که یک برنامه کاربردی نرم‌افزاری است که با همان تهدیداتی روبرو خواهد بود که یک افزاره سخت‌افزاری اختصاص یافته با آن مواجه است. تنها تفاوتی که وجود دارد میزان وابستگی سرور احراز هویت به سکو زیرین برای کاهش تهدیدات به‌جای تکیه بر قابلیت‌های کارکردی خود است.

جدول ۲۱- تهدیدات

نام تهدید	تعریف تهدید
T.FALSE_ENDPOINTS	ممکن است یک عامل مخرب، خود را به‌جای محصول یا NAS جا بزند و موجب شود که محصول به روشی غیر ایمن عمل کند یا داده‌های مرتبط با امنیت را از محصول یا محیط عملیاتی آن استخراج کند.
T.INVALID_USERS	ممکن است یک کاربر مخرب از داده‌های اعتبارنامه‌ای نادرست یا دیگر درخواست‌های احراز هویت نامعتبر که توسط محصول تأییدشده یا نادیده گرفته شوند را تأمین کند، از این رو، منابع محافظت‌شده در محیط عملیاتی سوژه‌ای برای دسترسی احراز هویت نشده هستند.

۷-۱-۳-خط‌مشی‌های امنیتی سازمانی

برای این بسته الحاقی هیچ خط‌مشی امنیتی سازمانی تعریف‌شده‌ای وجود ندارد.

۷-۱-۴- تناظر تعریف مسئله امنیتی

جدول زیر برای نگاشت تهدیدات و مفروضات تعریف‌شده در این بسته الحاقی برای اهداف امنیتی تعریف شده یا شناسایی‌شده در این بسته الحاقی به‌کار رفته است.

جدول ۲۲- تناظر تعریف مسائل امنیتی

تهدید یا مفروضات	اهداف امنیتی	الزامات کارکرد امنیتی
T.FALSE_ENDPOINTS	OE.TRUSTEDNAS	FCS_EAP-TLS_EXT.1, FIA_PSK_EXT.1, FTP_ITC.1
T.INVALID_USERS	O.RADIUSCOMPLIANT, O.USERAUTH	FCO_NRO.1, FCO_NRR.1, FCS_RADIUS_EXT.1, FCS_RADSEC_EXT.1, FIA_AFL.1 (see 1.4.3.3), FIA_UAU.6, FTA_TSE.1
A.NAS	OE.NAS	N/A

۷-۲- اهداف امنیتی

۷-۲-۱-اهداف امنیتی برای محصول

جدول زیر اهداف امنیتی خاص سرور احراز هویت را در خود جای داده است.

جدول ۲۳ اهداف امنیتی برای محصول

نام هدف امنیتی	تعریف هدف امنیتی
O.RADIUSCOMPLIANT	محصول باید پروتکل RADIUS را مطابق با RFCهای کاربردپذیر پیاده‌سازی کند.
O.TRUSTEDNAS	محصول باید سازوکارهایی برای تسهیل احراز هویت دوطرفه با NAS در محیط عملیاتی ارائه دهد.
O.USERAUTH	محصول باید سازوکاری برای ارزیابی درخواست‌های احراز هویت RADIUS ارائه دهد و بر اساس داده‌های کاربردپذیری که در درخواست موجود هستند نسبت به پذیرش، رد یا چالش پیام درخواست تصمیم‌گیری کند.

۷-۲-۲- اهداف امنیتی برای محیط عملیاتی

جدول زیر اهداف امنیتی خاص محیط عملیاتی برای سرورهای احراز هویت را شامل می‌شود.

جدول ۲۴ اهداف امنیتی برای محیط عملیاتی

نام هدف امنیتی	تعریف هدف امنیتی
OE.NAS	درخواست‌های احراز هویت که برای اعتبارسنجی در اختیار محصول قرار می‌گیرند به‌صورت متمرکز توسط NAS جمع‌آوری‌شده و از طریق این مؤلفه به محصول منتقل می‌شود.

۷-۲-۳- تناظر اهداف امنیتی

تناظر میان الزامات کارکردی امنیت و اهداف امنیتی تعریف‌شده یا شناسایی‌شده در این بسته الحاقی در بخش ۴ ارائه شده‌اند.

۷-۳- توجیه الزامات کارکردی امنیت

جدول ۲۵ توجیهی برای الزاماتی که به‌طور صریح بیان شده است

الزامات کارکرد امنیتی	منطق
FCS_EAP-TLS_EXT.1	این الزامات کارکردی امنیت برای تعریف روش احراز هویت دوطرفه EAP-TLS ایجاد شدند که توسط محصول و NAS برای احراز هویت یکدیگر به کار می‌رود.
FCS_RADIUS_EXT.1	این الزامات کارکرد امنیتی توسعه‌یافته برای شناسایی درست توانایی محصول به‌منظور پیاده‌سازی پروتکل RADIUS ایجاد شدند.
FCS_RADSEC_EXT.1	این الزامات کارکرد امنیتی توسعه‌یافته برای شناسایی درست توانایی محصول به‌منظور پیاده‌سازی امنیت لایه انتقال (TLS) بر روی RADIUS ایجاد شده‌اند.
FIA_PSK_EXT.1	این الزامات کارکرد امنیتی برای تعریف ترکیبی از راز مشترک RADIUS ایجاد شده است که کانال ارتباطی میان محصول و NAS را ایمن می‌کند.

جدول ۲۶- توجیه وابستگی الزامات کارکرد امنیتی

الزامات کارکرد امنیتی	وابستگی	منطق
FCS_EAP-TLS_EXT.1	هیچ وابستگی وجود ندارد	قابل‌اجرا نیست
FCS_RADIUS_EXT.1	هیچ وابستگی وجود ندارد	قابل‌اجرا نیست
FCS_RADSEC_EXT.1	هیچ وابستگی وجود ندارد	قابل‌اجرا نیست
FIA_PSK_EXT.1	هیچ وابستگی وجود ندارد	قابل‌اجرا نیست

پیوست ۱ الزامات اختیاری

این بخش شامل الزامات اختیاری است که می‌توانند به صلاحدید نویسنده هدف امنیتی مورداستفاده قرار گیرند. اگر محصول قابلیت‌هایی ارائه دهد که با هر یک از این الزامات اختیاری کنترل می‌شوند نویسنده هدف امنیتی باید الزامات مرتبط را در هدف امنیتی بگنجاند. با این وجود، نیازی نیست محصول معتبر توابع توضیح داده شده توسط این الزامات را اجرا کند و نویسنده هدف امنیتی می‌تواند هر تابعی شرح داده‌شده توسط هدف امنیتی که محصول ارائه نمی‌دهد را حذف کند.

۱-۱- شناسایی و احراز هویت

۱-۱-۱- الزام کارکرد امنیتی شناسایی و احراز هویت - احراز هویت مجدد (FIA_UAU.6.1)

زمانی که محصول سازوکار احراز هویت اجرایی خود را ارائه می‌دهد، الزامات کارکرد امنیتی اختیاری زیر که شامل قفل اجرایی آغاز شده محصول (و به عنوان الزام کارکرد امنیتی شناسایی و احراز هویت – احراز هویت مجدد توسعه‌یافته.۲ (FIA_UAU_EXT.2)، الزام کارکرد امنیتی شناسایی و احراز هویت – شناسایی و احراز هویت کاربر (FIA_UIA_EXT.1) و الزام کارکرد امنیتی دسترسی به محصول – قفل کردن و خاتمه دادن نشست توسعه‌یافته.۱ (FTA_SSL_EXT.1) در پروفایل حفاظتی مشترک افزاره شبکه (NDcPP) تعریف شده است) است باید گنجانده شود. به دلیل اینکه محصول که به عنوان برنامه نرم‌افزار کاربردی پیاده‌سازی شده ممکن است متکی به سازوکار احراز هویت مدیریتی باشد که به‌جای اینکه توسط محصول ارائه شود، توسط سکوی زیرین ارائه شده است، الزامات کارکرد امنیتی باید اختیاری در نظر گرفته می‌شود.

شماره الزام	نام الزام
۳۳	احراز هویت مجدد۱

محصول باید کاربر اجرایی را تحت شرایطی مجدداً احراز هویت کند: زمانی که کاربر کلمه عبور خود را تغییر می‌دهد، [انتخاب: قفل محصول آغاز شده زیر (الزام کارکرد امنیتی دسترسی به محصول – قفل کردن و خاتمه دادن نشست (FTA - SSL))، [اختصاص: *شرایط دیگر*]، شرط دیگری وجود ندارد].

اقدامات تضمین	
خلاصه مشخصه محصول (TSS)	ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا اطمینان حاصل کند، خط‌مشی‌های احراز هویت مجدد در آن گنجانده شده است و اینکه شرایط مورد نیاز احراز هویت مجدد و اقداماتی که هنگام رویارویی با این شرایط باید اتخاذ شود به‌خوبی تعریف شده است.
سند راهنمای اجرایی (AGD)	ارزیاب باید راهنماهای عملیاتی را مورد بررسی قرار دهد تا تعیین کند که راهنمایی‌هایی برای مدیران سیستم در مورد شرایطی که نیاز به احراز هویت مجدد کاربر است و اقداماتی که در صورت نیاز باید توسط مدیر سیستم اتخاذ شود ارائه داده است.
آزمون (Test)	ارزیاب باید آزمون‌های زیر را برای هر روشی که مدیران سیستم راه دور با آن به محصول دسترسی دارند انجام دهد. آزمون ۱: ارزیاب باید تلاش کند تا کلمه‌های عبور آنان را به همان شکلی تغییر دهد که در راهنمای عملیاتی دستور داده شده است. هنگام انجام چنین تلاشی، ارزیاب باید بررسی کند که احراز هویت مجدد لازم شده است یا خیر. آزمون ۲: ارزیاب باید تلاش کند تا تحت هر یک از شرایط باقیمانده مشخص شده در الزام به سامانه وارد شود. هنگام انجام چنین تلاشی، ارزیاب باید بررسی کند که احراز هویت مجدد لازم شده است یا خیر.

پیوست ۲ الزامات مبتنی بر انتخاب

بخش زیر شامل الزامات کارکرد امنیتی است که با توجه به انتخاب‌های انجام‌گرفته در بخش ۵ مورداستفاده قرار می‌گیرند.

۲-۱- پشتیبانی رمزنگاری

۲-۱-۱-الزام کارکردی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال (EAP-TLS)

اگر هرکدام از دنباله‌های رمز استفاده کننده از منحنی‌های بیضوی در الزام کارکردی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال توسعه‌یافته ۱,۱ (FCS_EAP-TLS_EXT.1.1) یا الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۳ (FCS_RADSEC_EXT.1.3) انتخاب شوند الزامات کارکرد امنیتی شماره ۱ زیر باید در هدف امنیتی گنجانده شوند.

۲-۱-۲- الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec) توسعه‌یافته.۱ (FCS_RADSEC_EXT.1)

اگر امنیت خدمت RadSec در الزام کارکرد امنیتی مسیر یا کانال امن – کانال امن درونی محصول (FTP_ITC.1) انتخاب شود الزامات کارکرد امنیتی شماره ۲ زیر باید در هدف امنیتی گنجانده شوند.

شماره الزام	نام الزام
۳۴	**پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال ۷**
محصول باید بسط منحنی‌های بیضوی پشتیبانی شده را در جواب آغاز ارتباط (Hello) سرویس گیرنده با منحنی‌های مؤسسه ملی استاندارد و فنّاوری[۴۶] (NIST) ارائه دهد: [انتخاب: secp256r1، secp384r1، secp521r1] و نه هیچ منحنی دیگری.	

[۴۶] National Institute of Standards and Technology

نکته کاربردی ۱۶: این الزام منحنی‌های بیضوی مجاز برای احراز هویت و توافق کلید برای منحنی مؤسسه ملی استاندارد و فنّاوری (NIST) از الزام کارکرد امنیتی پشتیبانی رمزنگاری- عملیات رمزنگاری: امضا کردن (*FCS_COP.1(3)*) و الزام کارکرد امنیتی پشتیبانی رمزنگاری –تولید کلیدهای رمزنگاری برای کلیدهای متقارن (*FCS_CKM.1(1)*) و الزام کارکرد امنیتی پشتیبانی رمزنگاری – توزیع کلید رمزنگاری (*FCS_CKM.2(1)*) را محدود می‌کند. این بسط برای دنباله رمزهای منحنی بیضوی پشتیبانی کننده سرویس گیرنده مورد نیاز است.

۳۵	**پروتکل امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec) توسعه‌یافته ۱**
محصول برای ارتباط امن با NAS باید امنیت خدمت RadSec را به همان شکل مشخص‌شده در RFC 6614 توسعه دهد.	
۳۶	**پروتکل امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec) توسعه‌یافته ۲**
محصول باید احراز هویت نظیر[۴۷] را با استفاده از [انتخاب: گواهی‌نامه‌های X.509v3، کلیدهای از قبل به اشتراک گذاشته شده] انجام دهد.	
۳۷	**پروتکل امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec) توسعه‌یافته ۳**

محصول باید نسخه ۱٫۱ امنیت لایه انتقال (TLS) یا نسخه‌های بعدی که از سامانه‌های رمزنگاری زیر پشتیبانی می‌کنند را پیاده‌سازی کند:

[انتخاب: دنباله رمز اجباری برای گواهی‌نامه‌های X509v3:

- TLS_RSA_WITH_AES_128_CBC_SHA

،

دنباله رمز اجباری برای کلیدهای از قبل به اشتراک گذاشته شده:

- TLS_PSK_WITH_AES_128_CBC_SHA]

[انتخاب: دنباله رمزهای اختیاری برای گواهی‌نامه‌های X509v3:

[۴۷] Peer

[انتخاب:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- هیچ دنباله رمز دیگری

]،

دنباله رمزهای اختیاری برای کلیدهای از قبل به اشتراک گذاشته شده:

[انتخاب:

- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA

- TLS_RSA_PSK_WITH_AES_128_CBC_SHA - TLS_RSA_PSK_WITH_AES_256_CBC_SHA - هیچ دنباله رمز دیگری]]	
پروتکل امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec) توسعه‌یافته ۴	**۳۸**
اگر دنباله رمز اختیاری برای کلیدهای از قبل به اشتراک گذاشته شده در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۳ (FCS_RADSEC_EXT.1.3) انتخاب شود، محصول باید قادر به [انتخاب: پذیرش، تولید با استفاده از تولیدکننده بیت تصادفی توصیف‌شده در الزام کارکرد امنیتی پشتیبانی رمزنگاری - تولید بیت تصادفی توسعه‌یافته.۱ (FCS_RBG_EXT.1)] کلیدهای از قبل به اشتراک گذاشته شده مبتنی بر بیت باشد. **نکته کاربردی ۱۷:** با این الزام دنباله‌های رمز اختیاری که باید در پیکربندی ارزیابی شده‌ای مورد آزمون قرار گیرند، محدود می‌شود. نویسنده هدف امنیتی باید دنباله رمز اختیاری را انتخاب کند که پشتیبانی می‌شود و اگر هیچ دنباله رمز پشتیبانی شده‌ای به‌جز مجموعه‌های اجباری وجود نداشته باشد، باید «هیچ» را انتخاب کند. محدود کردن دنباله‌های رمز قابل‌استفاده در پیکربندی ارزیابی شده به شکل قابل اجرا بر روی سرور در محیط آزمایش ضروری است. الگوریتم‌های مجموعه B که در بالا ذکر شده‌اند (*RFC 6460*) الگوریتم‌های ارجح برای پیاده‌سازی هستند. به‌منظور اطمینان از انطباق با *RFC5246* و *RFC 6614* به *TLS_RSA_WITH_AES_128_CBC_SHA* نیاز است.	

اقدامات تضمین

اقدامات تضمین الزام کارکردی پشتیبانی رمزنگاری پروتکل احراز هویت توسعه‌پذیر - امنیت لایه انتقال	
اقدامات موردنیاز برای پیگیری تحت الزام کارکردی امنیتی پشتیبانی رمزنگاری -پروتکل احراز هویت توسعه‌پذیر – امنیت لایه انتقال (FCS_EAP-TLS_EXT.1) در بخش ۵-۲-۲-۱ نشان داده شده‌اند.	
اقدامات تضمین الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده (RadSec) توسعه‌یافته	
خلاصه مشخصه محصول (TSS)	ارزیاب باید بررسی کند که توضیحات خلاصه مشخصه محصول شامل استفاده از RADIUS بر روی امنیت لایه انتقال (TLS) به همان شکل شرح داده شده در RFC 6614 باشد. اگر محصول از گواهی‌نامه‌های X.509v3 پشتیبانی می‌کند ارزیاب باید مطمئن شود که توضیحات خلاصه مشخصه محصول شامل استفاده از گواهی‌نامه‌های سمت سرویس گیرنده[۴۸] برای احراز هویت دوطرفه امنیت لایه انتقال (TLS) است. ارزیاب همچنین باید تأیید کند که توضیحات خلاصه مشخصه محصول نحوه مقایسه نام‌های متمایز[۴۹] (DN) یا نام‌های جایگزین موجودیت فعال[۵۰] (SAN) موجود در گواهی‌نامه با شناسه مورد انتظار را توضیح می‌دهد. ارزیاب باید توضیحات پیاده‌سازی پروتکل امنیت خدمت RadSec در خلاصه مشخصه محصول را برای اطمینان از مشخص شدن دنباله‌های رمز پشتیبانی شده بررسی کند. ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا از یکسانی دنباله‌های رمز مشخص‌شده با مواردی که برای این مؤلفه فهرست شده‌اند اطمینان حاصل کند. ارزیاب همچنین باید تأیید کند که خلاصه مشخصه محصول توضیحات مربوط به انکار نسخه‌های قدیمی لایه سوکت امن[۵۱] (SSL) و امنیت لایه انتقال (TLS) را در خود جای داده است. اگر یک دنباله رمز اختیاری برای کلید از قبل به اشتراک گذاشته در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۳

[۴۸] Client-side

[۴۹] Distinguished name

[۵۰] Subject Alternative Names

[۵۱] Secure socket Layer

	(FCS_RADSEC_EXT.1.3) انتخاب شود ارزیاب باید خلاصه مشخصه محصول را بررسی کند تا از داشتن توضیحات مربوط به فرایند تولید کلیدهای از قبل به اشتراک گذاشته شده مبتنی بر بیت (درصورتی‌که محصول از این قابلیت کارکردی پشتیبانی کند) مطمئن شود و تأیید کند که این فرآیند از تولید کننده اعداد تصادفی (RBG) مشخص‌شده در الزام کارکرد امنیتی پشتیبانی رمزنگاری تولید بیت تصادفی توسعه‌یافته.۱ (FCS_RBG_EXT.1) استفاده می‌کند.
سند راهنمای اجرایی (AGD)	ارزیاب باید تأیید کند که هرگونه تنظیمات ضروری برای برآوردن الزام در راهنماها گنجانده شده است. ارزیاب باید بررسی کند راهنما شامل دستورالعمل‌هایی برای تنظیم گواهی‌نامه‌های احراز هویت دوطرفه امنیت لایه انتقال (TLS) است. اگر نام متمایز (DN) به‌صورت خودکار با نام دامنه یا نشانی پروتکل اینترنتی (IP)، نام کاربری یا آدرس ایمیل مقایسه نشود ارزیاب باید مطمئن شود که راهنما شامل تنظیماتی برای نام متمایز (DN) مورد انتظار یا سرور دایرکتوری برای اتصال است. همچنین ارزیاب باید مستندات راهنما را برای اطمینان از داشتن دستورالعمل‌هایی برای تنظیم محصول بررسی کند به‌طوری‌که امنیت لایه انتقال (TLS) مطابق با توضیحات موجود در خلاصه مشخصه محصول باشد (برای مثال، مجموعه دنباله رمزهای اعلام شده در محصول ممکن است برای برآوردن این الزامات محدود شوند). اگر دنباله رمز اختیاری برای کلیدهای از قبل به اشتراک گذاشته شده در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۳ (FCS_RADSEC_EXT.1.3) انتخاب شود، ارزیاب باید تأیید کند که راهنمای عملیاتی شامل دستورالعمل‌هایی برای واردکردن کلیدهای از قبل به اشتراک گذاشته شده مبتنی بر بیت یا تولید کلید از قبل به اشتراک گذاشته شده مبتنی بر بیت (هر دو این موارد) است.
آزمون (Test)	ارزیاب باید آزمون‌های زیر انجام دهد. آزمون ۱: ارزیاب باید برای برقراری نشست RADIUS بدون امنیت لایه انتقال (TLS) تلاش کند و تأیید کند محصول چنین درخواستی را پردازش نکرده و عدم پذیرش را به صادر کننده پیام اعلام می‌کند. آزمون ۲: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید سرور را برای ارسال درخواست گواهی به سرویس گیرنده تنظیم کند و تلاش کند اتصالی را بدون ارسال گواهی‌نامه از سرویس گیرنده ایجاد کند. ارزیاب باید تائید کند که این اتصال انکار می‌شود.

آزمون ۳: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید سرور را برای ارسال درخواست گواهی به سرویس گیرنده بدون الگوریتم امضا پشتیبانی شده مورداستفاده گواهی‌نامه سرویس گیرنده پیکربندی کند. ارزیاب باید تلاش کند با استفاده از گواهی‌نامه سرویس گیرنده اتصالی ایجاد کند و تائید کند که چنین اتصالی انکار می‌شود. آزمون ۴: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید نشان دهد که استفاده از گواهی‌نامه بدون مسیر صدور گواهینامه معتبر منجر به شکست تابع می‌شود. با استفاده از دستورالعمل اجرایی، ارزیاب باید یک گواهی‌نامه یا گواهی‌نامه‌های موردنیاز برای اعتبارسنجی گواهی‌نامه‌ای که باید در تابع استفاده شود را بارگذاری کرده و نشان دهد که تابع موفقیت‌آمیز بوده است. ارزیاب باید یکی از گواهی‌نامه‌ها را حذف کند و نشان دهد که تابع با شکست مواجه می‌شود. آزمون ۵: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید گواهی‌نامه سرویس گیرنده را که به هیچ مرجع صلاحیت‌دار صدور گواهی متصل نیست (مرجع صدور گواهی اصلی یا میانجی) در پیام درخواست گواهی‌نامه سرور ارائه دهد. ارزیاب باید تأیید کند تلاش برای برقراری این ارتباط با شکست مواجه شده است. آزمون ۶: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید گواهی‌نامه سرویس گیرنده را با هدف احراز هویت سرویس گیرنده در رشته کاربردی کلید توسعه‌یافته ارائه دهد و بررسی کند که سرور تلاش برای برقراری ارتباط را پذیرفته است. ارزیاب باید این آزمایش را در حالت بدون هدف احراز هویت سرویس گیرنده تکرار کند و تأیید کند که سرور تلاش برای برقراری ارتباط را رد می‌کند. در حالت ایده‌آل، دو گواهینامه باید یکسان باشند به‌جز در هدف احراز هویت سرویس گیرنده. آزمون ۷: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲	

	(FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید تغییرات زیر را بر روی ترافیک انجام دهد. ○ یک بایت را در گواهی‌نامه سرویس گیرنده تغییر دهد. ارزیاب باید تائید کند که سرور ارتباط را رد می‌کند. ○ یک بایت را در پیام دست دهی تأیید گواهی‌نامه سرویس گیرنده تغییر دهد. ارزیاب باید تأیید کند که سرور اتصال را قطع می‌کند. آزمون ۸: [شرطی] اگر گواهی‌نامه‌های X.509v3 در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شوند، ارزیاب باید یک گواهی‌نامه سرویس گیرنده با یک شناسه که با شناسه مورد انتظار همخوانی ندارد را برای سرور ارسال کند و تأیید کند که سرور ارتباط را رد می‌کند. آزمون ۹: [شرطی] اگر کلیدهای از قبل به اشتراک گذاشته در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۲ (FCS_RADSEC_EXT.1.2) انتخاب شود، ارزیاب باید یک کلید نامعتبر تولید کند و نشان دهد که سرویس گیرنده نمی‌تواند با استفاده از این کلید مراوده یک پروتکل را با موفقیت به پایان رساند. آزمون ۱۰: ارزیاب باید یک اتصال امنیت لایه انتقال (TLS) با استفاده از دنباله‌های رمز مشخص‌شده در الزام برقرار کند. این اتصال ممکن است به‌عنوان قسمتی از برقراری پروتکل سطح بالاتر برقرار شود برای مثال، به‌عنوان قسمتی از نشست پروتکل امن انتقال ابرمتن (HTTPS). مشاهده مراوده موفق یک دنباله رمز برای برآورده ساختن هدف آزمون کافی است. بررسی مشخصات ترافیک رمزگذاری شده در تلاش برای تشخیص دنباله رمزهای مورد استفاده ضروری نیست (برای مثال، این‌که الگوریتم رمزنگاری استاندارد رمزگذاری پیشرفته[۵۲] (AES) ۱۲۸ بیتی است و استاندارد رمزگذاری پیشرفته (AES)۲۵۶ بیتی نیست). آزمون ۱۱: ارزیاب باید پیام آغاز ارتباط (Hello) سرویس گیرنده را با فهرستی از دنباله‌های رمزی به سرور بفرستد که شامل هیچ‌کدام از دنباله‌های رمز موجود در سرورهای هدف امنیتی نیست و تأیید کند که سرور اتصال را رد می‌کند. علاوه بر این، ارزیاب باید پیام آغاز ارتباط (Hello) سرویس گیرنده را به سروری که فقط دنباله رمز TLS_NULL_WITH_NULL_NULL را دارد بفرستد و تأیید کند که سرور اتصال را رد می‌کند.

[۵۲] Advanced Encryption Standard

	آزمون ۱۲: ارزیاب باید از یک سرویس گیرنده برای ارسال یک پیام تبادل کلید در اتصال امنیت لایه انتقال (TLS) استفاده کند که این کلید با دنباله رمز انتخابی سرور مطابقت ندارد (برای مثال، ارسال کلید تبادل دیف – هلمن منحنی بیضوی[۵۳] (ECDHE) در حالی‌که از دنباله رمز TLS_RSA_WITH_AES_128_CBC_SHA استفاده می‌کند یا ارسال کلید تبادل رایوست-شامیر-ادلمن (RSA) درحالی‌که از دنباله رمزهای الگوریتم امضای دیجیتال منحنی بیضوی[۵۴] (ECDSA) استفاده می‌کند). ارزیاب باید تأیید کند که سرور بعد از دریافت پیام تبادل کلید ارتباط خود را قطع می‌کند. آزمون ۱۳: ارزیاب باید تغییرات زیر را بر روی ترافیک انجام دهد: ○ در یک بایت از مقدار مقطعی[۵۵] سرویس گیرنده موجود در پیام دست دهی آغاز ارتباط (Hello) سرویس گیرنده تغییر ایجاد کرده و تائید کند که سرور پیام دست دهی تأیید گواهی‌نامه را رد خواهد کرد (اگر از احراز هویت دوطرفه استفاده می‌شود) یا سرور پیام دست دهی پایان‌یافته سرویس گیرنده را رد می‌کند. ○ قالب امضا در پیام دست دهی تبادل کلید سرویس گیرنده را تغییر داد و تائید کند که پیام دست دهی تائید گواهی‌نامه سرویس گیرنده توسط سرور رد شده است (اگر از احراز هویت دوطرفه استفاده می‌شود) یا سرور پیام دست دهی پایان‌یافته سرویس گیرنده را رد می‌کند. ○ یک بایت در پیام دست‌دهی پایان‌یافته سرویس گیرنده را تغییر داده و تائید کند که سرور اتصال را رد می‌کند و داده کاربردی را ارسال نمی‌کند. ○ بعد از تولید هشدار جدی[۵۶] با ارسال پیام پایان‌یافته از طرف سرویس گیرنده قبل از اینکه سرویس گیرنده پیام تغییر مشخصات رمز[۵۷] را ارسال کند، پیام آغاز ارتباط (Hello) سرویس گیرنده را با شناسه نشست از آزمون قبلی ارسال کند و تائید کند که سرور اتصال را رد می‌کند. ○ بعد از اینکه سرویس گیرنده پیام تغییر مشخصات رمز را صادر کرد یک پیام درهم[۵۸] از طرف سرویس گیرنده ارسال می‌کند و تائید می‌کند که

[۵۳] elliptic curve diffie-hellman key exchange

[۵۴] Elliptic Curve Digital Signature Algorithm

[۵۵] Nonce

[۵۶] Fatal Alert

[۵۷] ChangeCipherSpec

	سرور اتصال را رد می‌کند. آزمون ۱۴: ارزیاب باید پیام آغاز ارتباط (Hello) سرویس گیرنده درخواست‌کننده یک اتصال با نسخه ۱,۰ لایه سوکت امن (SSL 1.0) ارسال کند و تأیید نماید که سرور ارتباط را رد می‌کند. ارزیاب باید این آزمون را با نسخه‌های ۲,۰، ۳,۰ لایه سوکت امن (SSL 2.0، SSL 3.0)، نسخه ۱,۰ امنیت لایه انتقال (TLS 1.0) و دیگر نسخه‌های انتخاب‌نشده امنیت لایه انتقال (TLS) تکرار کند. آزمون ۱۵: [شرطی] اگر دنباله رمز اختیاری با استفاده از کلیدهای از قبل به اشتراک گذاشته شده در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۳ (FCS_RADSEC_EXT.1.3) انتخاب شوند و محصول کلیدهای از قبل به اشتراک گذاشته شده مبتنی بر بیت را تولید نکند ارزیاب باید کلید از قبل به اشتراک گذاشته شده مبتنی بر بیت با طول مناسب را به دست آورد و آن را با توجه به دستورالعمل‌های راهنمای عملیاتی وارد کند. ارزیاب باید نشان دهد که مراوده پروتکل موفق می‌تواند با استفاده از کلید انجام شوند. آزمون ۱۶: [شرطی] اگر دنباله رمز اختیاری با استفاده از کلیدهای از قبل به اشتراک گذاشته شده در الزام کارکردی پشتیبانی رمزنگاری پروتکل امنیت خدمت RadSec توسعه‌یافته.۱,۳ (FCS_RADSEC_EXT.1.3) انتخاب شوند و محصول کلیدهای از قبل به اشتراک گذاشته شده مبتنی بر بیت را تولید کند ارزیاب

[۵۸] Garbled Message

	باید کلید از قبل به اشتراک گذاشته شده مبتنی بر بیت با طول مناسب را تولید کرده و با توجه به دستورالعمل‌های راهنمای عملیاتی از آن استفاده کند. ارزیاب باید نشان دهد که مراوده پروتکل موفق می‌تواند با استفاده از کلید انجام شوند.

پیوست ۳ الزامات هدف

این بخش برای الزاماتی است که فعلاً در این بسته الحاقی به آن‌ها پرداخته نشده است ولی انتظار می‌رود در نسخه‌های آتی بسته الحاقی گنجانده شوند. فروشندگانی که جهت اجرای ارزیابی برای محصولات آینده برنامه‌ریزی می‌کنند، جهت برنامه‌ریزی برای برآوردن این الزامات هدف مورد تشویق هستند.

در حال حاضر هیچ الزامات هدفی برای این بسته الحاقی تعریف نشده است.

پیوست ۴ نمادها و اختصارات

نماد	معادل انگلیسی	معادل فارسی
AAA	Authentication, Authorization and Accounting	احراز هویت، اعطای مجوز و حسابرسی
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
AGD	Administrative guidance document	سند راهنمای اجرایی
App PP	Application Software Protection Profile	پروفایل حفاظتی برنامه کاربردی
CA	Certificate Authority	صلاحیت‌دار صدور گواهی
CCRA	Common Criteria Recognition Arrangement	توافقنامه به رسمیت شناختن معیار مشترک
CHAP	Challenge Handshake Authentication Protocol	پروتکل احراز هویت دست‌دهی چالش
DN	Distinguished name	نام‌های متمایز
EAP	Extensible Authentication Protocol	پروتکل احراز هویت توسعه‌پذیر
ECDHE	elliptic curve diffie-hellman key exchange	ارسال کلید تبادل دیف – هلمن منحنی بیضوی
ECDSA	Elliptic Curve Digital Signature Algorithm	الگوریتم امضای دیجیتال منحنی بیضوی
EP	Extended Package	بسته الحاقی
FIPS	Federal Information Processing Standard	استاندارد پردازش اطلاعات فدرال
HTTPS	Hypertext Transfer Protocol Secure	پروتکل امن انتقال ابرمتن
IETF	Internet Engineering Task Force	نیروی ضربت مهندسی اینترنت
IPsec	Internet Protocol Security	امنیت پروتکل اینترنت
MD5	message-digest algorithm	الگوریتم خلاصه پیام

NaK	Negative-Acknowledgement	تصدیق منفی
NAS	Network Access Server	سرور دسترسی شبکه
NDcPP	Network Device Collaborative Protection Profile	پروفایل حفاظتی مشارکتی افزاره شبکه
NIST	National Institute of Standards and Technology	مؤسسه ملی استاندارد و فنّاوری
RADIUS	Remote Authentication Dial In User Service	خدمت احراز هویت از راه دور کاربران تماس‌گیرنده
RadSec	RADIUS security over TCP and TLS	امنیت خدمت احراز هویت از راه دور کاربر تماس‌گیرنده
RBG	Random Bit generator	تولید کننده بیت تصادفی
RFC	Request For Comment	درخواست برای تفسیر
RSA	Rivest-Shamir-Adleman cryptosystem	سیستم رمزنگاری رایوست، شامیر، ادلمن
SAN	Subject Alternative Names	نام‌های جایگزین موجودیت فعال
SAR	security assurance requirements	الزامات تضمین امنیتی
SFR	security functional requirements	الزامات کارکرد امنیتی
SSH	Secure shell protocol	پروتکل پوسته امن
SSL	Secure socket Layer	لایه سوکت امن
TLS	Transport Layer Security	امنیت لایه انتقال
TSS	TOE Summary Specification/TSS	خلاصه مشخصه محصول
VPN	Virtual Private Network	شبکه خصوصی مجازی
WLAN	Wireless Local Area Network	شبکه محلی بی‌سیم