|  |  |
| --- | --- |
| عنوان پروژه | توسعه آزمايشگاه‌هاي تخصصي امنيتي جهت ارزيابي امنیت و کارکرد/کارایی NG-Firewall |
| پژوهشكده | امنيت ارتباطات و فناوري اطلاعات |
| گروه | امنیت شبکه |
| تاريخ |  |

**مقدمه** (شامل انگيزه تعريف پروژه و سوابق آن):

ارزیابی محصولات شبکه و به‌صورت خاص محصولات حوزه امنیت شبکه، به‌دلیل اهمیت کاربردهای این محصولات در بخش‌های حساس و حیاتی، از اهمیت ویژهای برخوردار است. ارزیابی این محصولات هم برای توسعه‌دهندگان محصول و هم برای کاربران حوزه‌های مختلف این محصولات، تاییدپذیری و اطمینان را بدنبال دارد. استانداردهای سری ISO 15408 در آزمایشگاههای CC در نقاط مختلف دنیا بعنوان مرجع ارزیابی و ارائه گواهی سطوح مختلف تایید امنیتی برای محصولات این حوزه مطرح می‌باشند. در این پروژه سعی بر این است تا براساس استاندارد مذکور و شاخص‌های برگزیده کارکرد/کارایی، محصولات در دسته دیواره آتش نسل بعدی (NGFW) مورد ارزیابی امنیتی و ارزیابی کارکرد/کارایی قرار گیرند.

در حال حاضر در پژوهشگاه ارتباطات و فناوری اطلاعات، آزمایشگاه امنیت با هدف ارائه خدمات تخصصی متناسب با نیاز کشور و همگام با رشد فناوری و همچنین تولید ملی و بومی‌سازی با اتکا به دانش پژوهشگران و متخصصان داخلی در حوزه افتا فعالیت می‌نماید. این آزمایشگاه دارای گواهی‌نامه ارائه خدمات امنیتی در سه حوزه، برنامه‌های کاربردی - تجهیزات شبکه - تجهیزات صنعتی سایبری (اولین آزمایشگاه مرجع کشور جهت ارائه خدمات ارزیابی امنیت در حوزه صنعت) می‌باشد.

1. **هدف پروژه:**

با توجه به مطالعات و بررسی‌های انجام شده و بررسی نیازهای کشور متناسب با سیاست‌های برنامه توسعه و نیز همسویی با برنامه و ماموریت وزارت ارتباطات و سازمان‌های زیرمجموعه و اعلام نیاز بخش دولتی و خصوصی مانند (زیرساخت‌های حوزه انرژی (وزارت نیرو) و متقاضیان دریافت بخش خصوصی (تولید کننده‌های تجهیزات و محصولات بومی در داخل کشور)، دليل انجام اين پروژه توسعه زیرساخت آزمایشگاه فعلی جهت امکان ارائه خدمات امنیتی برای محصولات NGFW در سطح EAL-2 استاندارد CC و نیز ارتقاء سطح ارزيابي عملكردي و كارائي برای دو دسته محصول فوق‌الذکر است.

1. **تعاريف و اصطلاحات:**
2. استاندراد معیارهای مشترک[[1]](#footnote-1) (CC): استاندارد ارزیابی معیار مشترک برای ارزیابی امنیت فناوریهای اطلاعات مشتمل بر دو دسته الزامات کارکردی امنیت و الزامات تضمین امنیت که در بستر متدلوژی ارزیابی معیار مشترک برای ارزیابی امنیت محصولات فناوری‌های اطلاعات توسط آزمایشگاه ارزیابی معیارهای مشترک مورد استفاده قرار می‌گیرد.
3. سطح تضمین ارزیابی[[2]](#footnote-2) (EAL): مجموعه ای از الزامات تضمین که از قسمت سوم استاندارد «ارزیابی معیار مشترک» برگرفته شده و نشان دهنده سطح امنیتی محصول است. سطوح تضمین از سطح 1 تا سطح 7 هستند.
4. پروفایل حفاظتی[[3]](#footnote-3) (PP): مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات؛ مجموعه‌ای که مستقل از پیاده‌سازی است.
5. شاخص ارزیابی (اندازه‌گیری) کاراریی: پارامترهای قابل اندازه‌گیری کمی که برای بنچمارکینگ و بررسی عملکرد محصولات فناوری اطلاعات در حوزه‌های مختلف توسط آزمایشگاه های مرجع مورد استفاده قرار می‌گیرند.
6. آزمایشگاه ارزیابی معیارهای مشترک: در چارچوب طرح ارزیابی و اعتبارسنجی معیارهای مشترک (CCEVS)، یک مرکز ارزیابی امنیت فناوری اطلاعات، مورد تایید مرکز راهبردی افتا برای انجام ارزیابی‌های مبتنی بر معیارهای مشترک.
7. **قلمرو پروژه** (شامل مشتري پروژه، قلمرو منطقي، قلمرو فيزيکي، فناوري مورداستفاده و ساير الزامات نظير مشخصات فني)**:**

طراحي آزمايشگاه براساس زیرساخت موجود در آزمایشگاه امنیت پژوهشگاه و محدود به انجام آزمون‌های کارکرد/کارایی و امنیتی بسته به محصول مورد نظر مطابق با استاندارد Common Criteria يا دیگر استانداردهاي مربوطه به ویژه در بخش کارکرد و کارایی است. در این راستا طراحی و پیاده‌سازی آزمایشگاه ارزيابي جهت آزمون کارایی محصولات بومی و غیربومی NGFW بر مبناي معيارهاي تدوین شده در پروژه و ارزيابي امنيتي بر اساس سطح تضمين 1 و 2 (EAL-1 EAL-2) براي محصولات مذکور صورت می‌پذیرد که لازم است سند پروفايل حفاظتي و روال‌های آزمون براي سطح تضمين 2 محصولات تدوین گردد.

1. **مراحل اجرا و شرح خدمات پروژه**

**مرحله اول: مطالعه و طراحی آزمایشگاه**

فعاليت‌هاي پیش‌بینی‌شده براي اين مرحله عبارت‌اند از :

* نهایی سازی تعریف محصول و بررسی و شناسایی کارکردهای سامانه NGFW در محصولات برتر جهانی
  + ارتباطات و مرزهای محصول
  + معماری و ساختار داخلی
  + کارکردهای اصلی و پشتیبان محصول
* تدوین مستندات تست کارکردهای امنیتی براساس CC
  + استخراج الزامات کارکردی امنیت براساس کاتالوگ الزامات معیارهای مشترک (CC) (در صورت نیاز تعریف کلاس‌ه الزامات کارکرد امنیتی متناظر با محصول NGFW):
    - تعریف و مدل سازی تهدیدات
    - استخراج اهداف امنیتی و ارائه دلایل کافی مبنی بر چگونگی پاسخ به تهدیدات
    - استخراج الزامات کارکردی امنیت و ارائه دلایل
  + تدوین سند پروفايل حفاظتي سطح EAL-2 براي سامانه NGFW
  + مستندات پشتیبان جهت اجرای تست الزامات کارکردی در سند پروفایل حفاظتی
    - مستندسازی روال تست (Test Method) الزامات کارکردی امنیت
    - فرایند آزمون محصولات NGFW در سطح EAL-2
    - تعریف نقش‌ها و مسئولیت‌ها
    - تمپلیت ارائه گزارش‌ها
* تدوین مستندات تست کارکرد و کارایی
  + تدوین پارامترهای و شاخص‌های (مقایسه[[4]](#footnote-4)) اصلی در ارزیابی عملکرد و کارایی
    - مطالعه و بررسي فرآيند آزمايشگاه‌هاي زبده جهان در ارزيابي عملكرد/کارایی محصول NGFW،
    - تدوین معيارها و موارد آزمون مورد استفاده در تست
  + ارائه طرح آزمایشگاه ارزیابی کارکرد و کارایی NGFW براساس بستر موجود در آزمايشگاه امنيت پژوهشکده
    - شناسایی وضعیت موجود
    - مستند طرح پیشنهادی آزمایشگاه
    - مستند سازی روال انجام تست کارایی و کارکرد
    - مستدسازی روش‌های گردآوری Data-Set
    - آماده سازی نسخه اولیه Data-Set

**مرحله دوم: پیاده سازی آزمايشگاه ارزيابي**

فعاليت‌هاي پیش‌بینی‌شده براي اين مرحله عبارت‌اند از :

* تجهیز و استقرار فرایندهای آزمایشگاه ارزیابی امنیتی
  + نصب ابزارهاي لازم
  + پیاده سازی فرایندهای آزمون امنیتی
    - استقرار و آموزش پرسنل
    - پیاده سازی روال های تست
    - پیاده سازی قالب ارائه گزارش
  + تدوین مستندات راهنمای توسعه‌دهندگان (ارائه‌دهندگان) محصول به آزمایشگاه
* آزمایشگاه تست کارایی/کارکرد
  + راه‌اندازي اوليه زيرساخت آزمايشگاه و ابزارهاي آزمون ارزيابي عملكردي
  + پیاده سازی فرایندهای آزمون
    - استقرار و آموزش پرسنل
    - پیاده سازی روال های تست
    - پیاده سازی قالب ارائه گزارش
  + تدوین مستندات راهنمای توسعه‌دهندگان (ارائه‌دهندگان) محصول به آزمایشگاه ارزیابی عملکرد

1. **خروجي‌هاي هر مرحله از اجراي پروژه**

خروجي‌هاي پیش‌بینی‌شده براي هر يک از مراحل اجراي پروژه، عبارت‌اند از :

**خروجي‌هاي مرحله اول:**

1. گزارش مطالعاتی شناسایی عملکردهای اصلی سامانه‌های NGFW
2. پروفايل حفاظتي سطح 2 براي محصولات NGFW
3. مستند متد انجام تست الزامات کارکرد امنیتی NGFW
4. مستند متد انجام تست کارایی و کارکرد محصولات NGFW
5. مستند طراحی آزمایشگاه ارزیابی کارایی و کارکرد NGFW

**خروجي‌هاي مرحله دوم:**

1. آزمایشگاه ارزیابی امنیتی
2. آزمایشگاه تست کارکرد/کارایی
3. مستند راهنمای ارائه دهندگان محصول به آزمایشگاه (ارزیابی امنیتی و تست کارکرد/کارایی)
4. **حداکثر مدت‌زمان مجاز و اعتبار براي ارائه پيشنهاد و اجراي پروژه** 
   * **حداکثر مدت‌زمان مجاز براي ارائه پيشنهاد:**

دريافت‌کننده RFP، مي‌بايست حداکثر 14 روز پس از دريافت RFP، پيشنهاد خود را بر اساس مکانیسم پیش‌بینی‌شده دربند 8 اين RFP، تحويل مرکز تحقيقات مخابرات ايران نمايد. پیشنهاد‌های ارائه‌شده پس‌ازاین تاريخ، قابل وصول توسط مرکز تحقيقات مخابرات ايران نخواهند بود.

* + **حداکثر مدت‌زمان مجاز براي اجراي پروژه:**

حداکثر مدت‌زمان پیش‌بینی‌شده و قابل‌پذيرش براي اجراي اين پروژه، 6 ماه مي‌باشد. چنانچه پيشنهاددهنده در فرم پيشنهاد پروژه، مدت‌زمان اجراي پروژه را بيش از مدت‌زمان مجاز اعلام نمايد، قابل وصول توسط مرکز تحقيقات مخابرات ايران نخواهد بود.

1. **ساير الزامات و محدوديت‌هاي موجود در اجراي پروژه**

علاوه بر محدوديت موجود در خصوص زمان اجراي پروژه، لازم است پیشنهاددهندگان در تنظيم پيشنهاد خود، موارد ذيل را نيز رعايت فرمايند :

1. پيشنهاد بايد در قالب آخرين نسخه از "فرم پيشنهاد پروژه" موجود در سايت مرکز تحقيقات مخابرات ايران (حوزه معاونت پژوهش و توسعه ارتباطات علمي، دفتر امور پژوهشي، فرم‌ها )، تنظيم و ارائه گردد.
2. در جدول ساختار شکست پروژه پیش‌بینی‌شده در بخش 2-3-7 فرم پيشنهاد پروژه، لازم است شرح فعاليت‌هاي هر مرحله از پروژه (مطابق شرح فعاليت‌هاي پیش‌بینی‌شده در RFP به همراه موارد احتمالي که پیشنهاددهنده، انجام آن‌ها را ضروري مي‌داند) به همراه کليه اطلاعات درخواست شده در فرم، به تفکيک براي هر فعاليت و مرحله، ارائه گردد. از خالي گذاشتن ستون‌هاي اين جدول براي فعاليت‌هاي پروژه، خودداري گردد.
3. در جدول مشخصات منابع انساني پیش‌بینی‌شده در بخش 3-1 فرم پيشنهاد پروژه، لازم است نام و ساير مشخصات درخواست شده براي کليه پرسنلي که در اجراي پروژه به‌صورت واقعي مشاركت دارند با ذكر ميزان مشاركت درج گردد.
4. هزينه‌هاي سربار، تنها براي پيشنهاددهندگان حقوقي ( دانشگاه‌ها ) پیش‌بینی‌شده است و شرکت‌ها مي­توانند بجاي هزینه سربار، هزينه­هاي اضافي متحملِ بابت اين پروژه را عنوان نمايند.
5. پيشنهاد سود خالص براي شركت­هاي خصوصي .
6. **تحويل پيشنهاد به مرکز تحقيقات مخابرات ايران**
   * **حداقل شرايط پيشنهاد قابل تحويل:**

پیشنهاد‌هایی قابل وصول مي‌باشند که شرايط مندرج دربندهای 6 و 7 اين RFP را کاملاً رعايت نموده باشند. در زمان ارائه پيشنهاد به مرکز تحقيقات مخابرات ايران، رعايت شرايط مذکور، کنترل‌شده و در صورت عدم رعايت هر يک از موارد، از تحويل پيشنهاد، خودداري خواهد شد.

* + **نحوه تحويل پيشنهاد:**

پیشنهاددهندگان مي‌بايست پيشنهاد خود را به نام معاونت پژوهش و توسعه ارتباطات علمي به دبيرخانه پژوهشگاه ارتباطات و فناوري اطلاعات، تحويل داده و رسيد دريافت نمايند. (درصورتی‌که مدارك به ساير واحدهای ديگر پژوهشگاه تحويل داده شود در فراخوان ثبت نخواهد شد و اين پژوهشگاه در قبال آن هیچ‌گونه مسئوليتي ندارد)

1. **نحوه ارزيابي پيشنهاد**

ارزيابي پیشنهاد‌های رسيده بر اساس پارامترهاي زير خواهد بود:

* 1. ميزان تسلط به ابعاد و جوانب پروژه (امتياز اين رديف با توجه به سمينار ارائه‌شده توسط پیشنهاددهنده و نيز مطالب ارائه‌شده در فرم پيشنهاد پروژه در خصوص شرح خدمات، خروجي­ها، اهداف و . . . تعيين مي­گردد)
  2. نحوة تخصيص منابع انساني شامل كيفيت و كميت نيروها (رزومه و سابقه كاري لازم در ارتباط با انجام خدمات موردنیاز پروژه، تعداد و تناسب نيروها با توجه به حجم كار، نوع رابطه استخدامي نيروها بر اساس مدارك ارائه‌شده)
  3. كيفيت ساختار شكست پروژه متناسب با شرح خدمات و اهداف پروژه
  4. كيفيت ساختار سازماني پیش‌بینی‌شده براي انجام پروژه(تيم­هاي اجرايي، مديريت پروژه و...)
  5. ساختار و روال­هاي پیش‌بینی‌شده براي كنترل و مديريت پروژه و تأييد صحت خروجي­ها
  6. روال­ها، متدولوژي و استانداردهاي پيشنهادي براي اجراي شرح خدمات
  7. نحوه ارائه زمان‌بندی و پوشش كامل و به‌موقع شرح خدمات
  8. مبلغ پيشنهادي

1. Common Criteria [↑](#footnote-ref-1)
2. Evaluation Assurance Level [↑](#footnote-ref-2)
3. Protection Profile [↑](#footnote-ref-3)
4. Benchmarking [↑](#footnote-ref-4)