. بسمه تعالی .

خرید، نصب و راه اندازی، آموزش و پشتیبانی یکساله

سیستم مدیریت یکپارچه تهدیدات - فایروال نسل بعدی

"Next Generation Firewall-UTM"

۱ - این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

فایروال درخواستی باید دارای قابلیت های ذیل باشد.

دارای تاییدیه افتا با اعتبار فعال

دارای گواهی ثبت فنی نرم افزار

دارای تاییدیه دانش بنیان در حوزه فناور

دارای تاییدیه سمتا

دارای تاییدیه پدافند غیرعامل

- خدمات پشتیبانی استاندارد
- خدمات مبتی بر تیکت
- تماس های دوره ای
- سرویس کلاد
- ارائه فایل راهنما و مستندات راهبری
- نصب و راه اندازی رایگان
- بروزرسانی آنلاین محصولات
- بروزرسانی آفلاین محصولات
- بررسی های مستمر و دوره ای بهینه سازی تنظیمات
- آموزش رایگان

۲ - این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

قابلیت های عمومی محصول:

۱. **امکانات مدیریتی:**

- ✓ پشتیبانی از تاریخ شمسی
- ✓ پشتیبانی از پیغام‌های مختلف
- ✓ پشتیبانی از زبان‌های فارسی، انگلیسی
- ✓ واسط مدیریتی نرم‌افزاریGUI
- ✓ واسط مدیریتیCLI
- ✓ مدیریت رمز عبور مدیر سیستم
- ✓ تعیین سطح دسترسی کاربران
- ✓ مدیریت گواهی‌نامه‌ها
- ✓ قابلیت CA Mgmt و ساخت گواهینامه‌هایSelf-signed
- ✓ ارائه پیغام به مدیر سیستم قبل از ورود به سیستم
- ✓ قفل‌کردن و خاتمه اتصال به سیستم
- ✓ قابلیت پشتیبان‌گیری خودکار بر روی دستگاه و همچنین سرورهای جانبی
- ✓ قابلیت پشتیبان‌گیری ابری
- ✓ قابلیت رمزگذاری بر روی فایل‌های پشتیبان
- ✓ امکان تعامل APIبا SIEM و تجهیزاتامنیتی مشابه
- ✓ به‌روزرسانی آنلاین
- ✓ به‌روزرسانی آفلاین

۲. **زیرسیستم تشخیص و جلوگیری از حملات (IDS / IPS)**

- ✓ قابلیتIDPS بومی (عدم استفاده از IDPSهای متن‌باز ازجمله Snort و Suricata)
- ✓ قابلیت اعمال محدودیت سرویس بر روی پروتکل‌های لایه ۷ در IDPS
- ✓ قابلیتیادگیری هوشمند
- ✓ قابلیتAnti-spoof در IDPS
- ✓ قابلیت تشخیص اسکنرها در IDPS
- ✓ امکان تعریف الگوهای شخصی به‌صورت دستی
- ✓ تعبیه الگوهای دسته‌بندی شده پیشفرض
- ✓ ثبت لاگ تفکیک‌شده

۳. **زیرسیستم دیواره آتش و امنیت (Firewall Security)**

- ✓ قابلیت عملکرد با و بدونZone بندی
- ✓ امکان پردازش پروتکل‌های خاص و انواع پروتکل های شبکه، پروتکل های لایه انتقال
- ✓ قابلیت حذف بسته ها قبل از بارگذاری کامل سیستم
- ✓ قابلیت تعریفFirewall Policyهای نامحدود به‌صورت شناسه محور
- ✓ قابلیت اعمال عملکرد Allow، Deny، Reject، Tarpit، Hijack، Monitor
- ✓ قابلیت پالیسی نویسی بر اساس نام کاربر، گروه، Reseller و ...

- ✓ قابلیت پشتیبانیاز SNAT و DNAT (شفاف و غیرشفاف) بر رویInterface، Balancerو IPبه همراه IP NAT Pool
- ✓ قابلیت پشتیبانی از NAT Pool با الگوریتمRandom، Rotary، Source، Destination
- ✓ قابلیت پشتیبانی از Port Address Translation (PAT) بهصورت شفاف و غیرشفاف
- ✓ قابلیت تشخیص پروتکل‌ها در لایه کاربردPort Enforcement بدون وابستگی به IDPS
- ✓ قابلیت تشخیصنرم افزارها در لایه کاربردApplication Awairness بدون وابستگی به IDPS
- ✓ قابلیت جلوگیری از حملات نوعTCP Hole Punching، انواع Flood و ...
- ✓ قابلیتSSL Offloader جهت Publish نمودن وب سرورهایSSL (SSL to TCP، TCP to SSL، SSL to SSL)
- ✓ قابلیت پشتیبانی از PBRیاForce Routeبه تفکیکInput و Output و Multiple
- ✓ قابلیتISDBجهت تشخیص آدرس IP کمپانی های مشهور
- ✓ قابلیتGEO IP و تشخیص آدرس IP کشورها
- ✓ قابلیت Vendor Blocking جهت تعریف پالیسی های امنیتی صرفاً لایه ۲، بطور مجزا از پالیسی های اصلی فایروال
- ✓ قابلیت تشخیص و کنترلSYN Cookie و SYN Proxy
- ✓ قابلیت امنیت هوشمند به تفکیک هر پالیسی جهت جلوگیری از حملات
- ✓ قابلیت جلوگیری از حملات و حالات غیرطبیعیIP Security، مرتبط با پروتکل TCP، UDP، IDMP، FTP
- ✓ قابلیت جلوگیری از Broadcast/Multicast Packet
- ✓ قابلیت تنظیمTimeout برای پروتکل‌های مختلف TCP، UDP، ICMP، GRE، ESP و ...
- ✓ قابلیت اعمال محدودیت‌های ترافیکی به تفکیک هر Client، Session و Policy
- ✓ تغییر وضعیتICMP
- ✓ جلوگیری از عبور پکت هایLink Local، Experimental و Fragmented
- ✓ قابلیتDHCP Server و پشتیبانی ازDHCP Relay

۴. **<u>زیر سیستم کنترل نرم افزارهای کاربردی (Application Control)</u>**:

- ✓ کنترل Appها بر اساس Name، MD5-Hash، Path، Cert Serial No، Cert Subject
- ✓ کنترل APPها در ازای انواع Identityها و بصورت کاملا شناسه محور
- ✓ کنترلAppها بر اساسPattern،IP، DNS، Domain، Port
- ✓ اعمال محدودیت پهنای باند به تفکیکAppها
- ✓ اعمالHTTP Security بر رویAPPها
- ✓ تعبیه دسته‌بندی‌های اولیه
- ✓ ثبت لاگ برنامه‌های کاربردی از جمله فیلترشکن ها

۵. **<u>زیر سیستم پالایش وب (L7 and Web Filtering)</u>**:

- ✓ قابلیت فیلترینگ بر روی پروتکل HTTP
- ✓ قابلیت فیلترینگ بر رویSSL (بدون استفاده از Certificate جعلی)
- ✓ قابلیت فیلترینگ بر رویTLS (بدون استفاده از Certificate جعلی)
- ✓ قابلیت فیلترینگ بر روی نوع و محتوای فایل‌ها (مثال JavaScript، ActiveX و ...)
- ✓ قابلیت فیلترینگ پروتکل FTP و TFTP
- ✓ قابلیت فیلترینگ بر روی پروتکل SMTP
- ✓ قابلیت فیلترینگ بر روی داده اصلی
- ✓ قابلیت فیلتر نمودن کلیه نرم‌افزارهای فیلترینگ (ازجمله Free gate و Ultra-surf و ...)
- ✓ فیلترینگ محتوا بر اساس کلمات موجود در لیست سیاه

۴ - **این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.**

- ✓ کنترل محتوا در سطح لایه کاربرد
- ✓ تعبیه دسته‌بندی‌های اولیه

۶. **زیر سیستم جلوگیری از نشست اطلاعات (DLP)**

- ✓ اعمال پالیسی ها بصورت شناسه محور
- ✓ قابلیت جلوگیری از نشت اطلاعات در پروتکل های فاش
- ✓ قابلیت تعریف فایل و فرمت
- ✓ قابلیت تعیینContent Type
- ✓ قابلیت تعیینName
- ✓ قابلیتImport نمودن لیست

۷. **زیر سیستم بد افزار (Advertisement/Anti Malware/Phishing)**

- ✓ قابلیت جلوگیری از آدرس هایMalwareها(شامل Attacks، Spyware، Viruses، Bots، ...)
- ✓ قابلیت جلوگیری از آدرس های مرتبط با تبلیغات
- ✓ قابلیت جلوگیری از آدرس هایRansomware ها و C&C سرورها
- ✓ قابلیت جلوگیری از دسترسی به آدرس سایت‌های فیشینگ ایرانی و خارجی
- ✓ قابلیت جلوگیری از ماینینگ ارز دیجیتال
- ✓ جلوگیری از Coin Miner
- ✓ اعمال قابلیت در ازای انواع Identityها و بصورت کاملا شناسه محور
- ✓ تعبیه دسته‌بندی‌های اولیه
- ✓ عملکرد بر رویSSL

۸. **زیر سیستم مدیریت کاربران و احراز هویت (Accounting and Identity)**

- ✓ قابلیت احراز هویت کاربران در مدل NATو Routeبدون نیاز به نصب هرگونه AgentیاDialerیاVPN در سمت کاربر
- ✓ قابلیت احراز هویت کاربران در مدل Layer 2 Bridge بدون نیاز به نصب هرگونه AgentیاVPN در سمت کاربر
- ✓ امکان ارتباط و اتصال به Radius
- ✓ قابلیت احراز هویت کاربران به روش NTLM، IP، MAC، Captive Portal، SSO، Basicدر تمامی مدل‌های عملیاتی L3 NAT، L3 Route و L2 Bridge
- ✓ قابلیت رمز نمودن اطلاعات کاربر در هنگام احراز هویت و احراز هویت در SSL
- ✓ هدایت کاربران به آدرس خاص
- ✓ پشتیبانی از قابلیتBYOD و اتصال هم‌زمان چند دستگاه برای کاربران
- ✓ قابلیت تغییر عنوان و لوگوی صفحه احراز هویت
- ✓ قابلیت اختصاری اتصال توسط Agent اختصاصی
- ✓ قطع خودکار اتصال کاربر
- ✓ قابلیت پشتیبانی از Domain Controllerهای مختلف (Trust و Untrusted)
- ✓ قابلیت به‌روزرسانی دامین به‌صورت خودکار
- ✓ جلوگیری از حمله Broute Force
- ✓ قابلیتImport نمودن لیست کاربران و گروه‌ها از Domainهای مختلف
- ✓ امکان اتصال به انواع Radius NAS Serverها
- ✓ تعریفRadius Reply list برای کاربران
- ✓ تعریفRadius Reply list برای گروه‌ها

۵ - **این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.**

- ✓ قابلیت اتصال به دیتابیس‌های مختلف (قابل انتخاب توسط کاربر)
- ✓ قابلیت اعمال محدودیت‌هایشناور مختلف زمانی، ترافیکی، حجمی بر روی کاربران و گروه‌ها
- ✓ قابلیت تعریفIdle Time out برای کاربران
- ✓ قابلیت اعمال پهنای باند Maximum و Warranty به کاربران و گروه‌ها
- ✓ قابلیت تخصیص منابع اضافی به کاربران و گروه‌ها
- ✓ قابلیت تعریف پیغام (Message) خودکار و زمان‌بندی‌شده
- ✓ قابلیت اتصال به SMS Server و احراز هویت (ثبت‌نام کاربران) از طریقSMS
- ✓ قابلیت وارد نمودن لیست شماره موبایل‌های مجاز
- ✓ عدم ذخیره رمز عبور کاربران واردشده از دامین
- ✓ امکان حذف اطلاعات قدیمی

۹. زیر سیستم موازنه بار (Balancing)

- ✓ قابلیتLink Balancing بر روی انواع ارتباطات (مانند Ethernet، Fiber، Wireless، ADSLو ...)
- ✓ قابلیتLink Balancing بر روی ارتباطات لاجیکال (ازجمله VPN، PPPOE و ...)
- ✓ قابلیت تعریف هم‌زمان انواع پالیسی هایLink Balancing به همراه Automatic Failover(TCP, DNS, ICMP)
- ✓ قابلیت تعریف هم‌زمان انواع پالیسی هایBalancing با الگوریتم‌های مبتنی بر کمترین بار ترافیکی، کمترین تعداد نشست‌ها، کمترین بایت ترافیکی، کمترین تعداد بسته‌ها، بهترین کیفیت، مبتنی بر مبدأ، مبتنی بر مقصد، کمترین زمان تأخیر، سریع‌ترین زمان پاسخ، الگوریتم تصادفی،الگوریتم چرخشییکتا، تشخیص اولین لینک سالم، سریع‌ترین زمان پاسخ
- ✓ قابلیتBalancing بر روی پروتکل SSL، VOIP

۱۰. زیر سیستم شبکه خصوصی مجازی (VPN)

- ✓ پشتیبانی از انواعVPN به‌صورت Client to Site شامل IPSec ، L2TP، PPTP
- ✓ قابلیتVPN به‌صورت Site to Site شامل GRE، GIF (IP in IP) و IPSec IKEv1|2
- ✓ قابلیت پشتیبانی از ارتباطات VPN اختصاصی SSL و لایه3
- ✓ امکان اتصال ارتباطات VPN به توکن های سخت افزاری و گواهینامه های امنیتی
- ✓ قابلیت DialUP-VPN و DMVPN

۱۱. زیر سیستم حفاظت از سرویس های وب

- ✓ شناسایی از مدلها و توانایی پردازشی متنوع
- ✓ تأیید اعتبار ورودی‌ها که درنتیجه ورود خطرناکSQL ، Cross-Site Scriptingو حملات پیمایشی دایرکتوری‌ها (Directory Traversal Attack)متوقف می‌گردد.
- ✓ شناساییCookie ، Sessionیا حملاتParameter Tampering
- ✓ Blockنمودن حملاتی که آسیب‌پذیری‌های موجود در دارایی‌های سفارشی تحت وب را Exploit می‌کنند
- ✓ جلوگیری از انتقال غیرمجاز داده‌های حساس از طریق شناسایی و Block کردن در سطحObject
- ✓ بررسی کامل ترافیک رمزگذاری شدهٔ SSL برای تمامی تهدیدات
- ✓ جلوگیری از تهدیدات فعال به‌واسطه Exploit نمودن نقاط ضعف منطقی در برنامه‌های سفارشی کسب‌وکار
- ✓ محافظت در برابر حملات Application-Layer Denial و حملاتDDoS
- ✓ پنهان نمودن اطلاعات واکنشی سرور که به طور بالقوه برای هکرها مفید می‌باشند
- ✓ ایجاد محافظت جامع و کامل از XML که دربرگیرنده اعتبار Schema برای پیام‌های SOAP و دفاع‌های ورودی XPath و همچنین شناساییبا Block نمودن فایل‌های ضمیمه XML با محتوای مخرب است
- ✓ ایجاد انطباق و سازگاری با شرایط ۶.۶ مربوط به Payment Card Industry Data Security Standardیا به‌اختصار

۶ - این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

- ✓ امکان حفاظت در مقابل حملات و آسیب پذیری های رایج منطبق بر OWASP Top10 2021 :
  - Broken Access Control، کنترل دسترسی کاربران طی مجوزهای صادره.
  - Cryptographic Failures، برای کشف اطلاعات حساس مالی، شخصی، اعتباری، اسرار تجاری و...
  - Injection از قبیلSQL ، NoSQL، OS، LDAPو...
  - Insecure Design، طراحی ناامن که ضمانت کد برنامه در برابر روش‌های شناخته شده حملات را تحت‌تأثیر قرار می‌دهد.
  - Security Misconfiguration برای دسترسی به اطلاعات از طریق پیکربندی نادرست و...
  - Vulnerable and Outdated Components برای دسترسی به اطلاعات مهم با استفاده از اجزای آسیب‌پذیری‌های شناخته‌شده در کامپوننت‌های نرم‌افزاری قدیمی و آسیب‌پذیر.
  - Identification and Authentication Failures که به مهاجمان اختیارات کافی برای به خطر انداختن رمزهای عبور، کلیدهایا توکن‌ها و ... را می‌دهند.
  - Insecure Software and Data Integrity Failures برای اجرای کد از راه دور و انجام حملات بعدی ازجمله حملات تزریق و حملات تشدید امتیاز و ... پیرو نقص‌های محافظت از یکپارچگی داده در کد یا زیرساخت برنامه
  - Security Logging and Monitoring Failures استخراج و نابودی اطلاعات و حمله به سایر سیستم‌ها به‌واسطه لاگینیا نظارت ناکافی
  - Server-Side Request Forgery (SSRF) در زمانی که یک برنامه کاربردی در حال واکشی کردن داده از یک منبع خارجی باشد و هیچ اعتبارسنجی رویURL ارائه شده توسط کاربر وجود نداشته باشد.

۱۲. زیر سیستم گزارش گیری (Report and Monitoring)

- ✓ قابلیت ثبت و فعال‌سازی لاگ پروتکل HTTP و HTTPS به تفکیک هر پالیسی
- ✓ قابلیت ثبت و فعال‌سازی لاگ Connections به تفکیک هر پالیسی
- ✓ قابلیت ثبت و فعال‌سازی لاگ DNS به تفکیک هر پالیسی
- ✓ نمایش گزارشات World Map
- ✓ قابلیت ثبت لاگ ها و نمایش گزارشات برحسب تاریخ شمسی
- ✓ قابلیت ثبت لاگ ها به فرمت CAP جهت Troubleshooting
- ✓ نمایش گزارشات مرتبط با سایت‌های مشاهده‌شدهبه‌صورت نموداری و مقداری
- ✓ نمایش گزارشات مرتبط با نشست‌ها به‌صورت نموداری و مقداری
- ✓ نمایش گزارشات مرتبط با حملات کشف شده توسط IDPS به‌صورت نموداری و مقداری
- ✓ نمایش گزارشات مرتبط با حملات کشف شده توسط WAF به‌صورت نموداری و مقداری
- ✓ نمایش گزارشات مرتبط با رخدادها و رویدادها به‌صورت نموداری و مقداری
- ✓ نمایش گزارشات مرتبط با میزان استفاده کاربران و گروه ها به‌صورت نموداری و مقداری
- ✓ گرفتن خروجی از گزارشات
- ✓ قابلیت پشتیبانی از Net flow v9وIPFixبه تفکیک هر پالیسی
- ✓ قابلیت ذخیره خودکار Logها در FTP Server
- ✓ قابلیت پشتیبانی از Syslog Server امن
- ✓ قابلیت ذخیره طولانی‌مدت لاگ ها در دستگاه
- ✓ قابلیت ثبت، نام کاربر در Session و URL log
- ✓ قابلیت نمایش آنلاین تمامی ارتباطات و کلاینت ها
- ✓ نمایش سایت‌های آنلاین در حال استفاده کلاینت ها

- این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

- ✓ قابلیت نمایش تغییرات انجام‌شده توسط مدیران سیستم
- ✓ قابلیت ارسال Alert به‌صورت ایمیلو SMSبه مدیران سیستم

۱۳. امکانات شبکه:

- ✓ قابلیت قرارگیری در مدهای عملیاتی L3 NAT، L3 Route و L2 Bridge به‌صورت هم‌زمان
- ✓ ارائه قابلیت‌های کامل NAT و Route در حالت L2 Bridge
- ✓ قابلیتSpan port
- ✓ قابلیت قرارگیری کارت شبکه‌ها در حالت Sniffer Mode
- ✓ ارائه خدمات Wi-Fi Access point
- ✓ قابلیت تعریفSub Interfaceهای نامحدود
- ✓ قابلیت پشتیبانی از VLAN
- ✓ قابلیت پشتیبانی از Ether channel (Link Aggregation) با الگوریتم‌های استاندارد
- ✓ پشتیبانی از Virtual IP
- ✓ پشتیبانی از Static Routing
- ✓ پشتیبانی از مسیریابی پویا
- ✓ ویرایشRouteها
- ✓ پشتیبانی از قابلیتDNS Forwarder و تعریفMaster listهای اختصاصی
- ✓ قابلیتBind کردن آدرس‌هایDNS خاص بر رویHostها
- ✓ پشتیبانی از High Availability به تعداد نامحدود و حداقل در حالت Active/Passive
- ✓ مدیریتARP
- ✓ تعریفIP نامحدود بر رویInterface
- ✓ قابلیتBind کردن IP به MAC

۱۴. امکانات امنیت SSL و TLS

- ✓ قابلیتتشخیصciphersهای ضعیف
- ✓ قابلیت تشخیص گواهینامه‌ها با Digest ضعیف
- ✓ قابلیت تشخیص گواهینامه‌های منقضی
- ✓ قابلیت تشخیص گواهینامه‌های شخصی
- ✓ قابلیت تشخیص گواهینامه‌هایSSL V2
- ✓ قابلیت تشخیص گواهینامه‌هایSSL V3
- ✓ قابلیت تشخیص گواهینامه‌هایTLS V1
- ✓ قابلیت تشخیصTLS Extension server name
- ✓ مکانیزم عملکردیSSL و TLS به‌صورت Drop-Log، Drop-Silent و Log Only

جدول ۱ - قابلیت های اختصاصی		
ردیف	مشخصات	توضیحات
1	**بروزرسانی آنلاین از سرورهای ایران، شامل:**	۱. بروزرسانی روزانه آدرس های IP/Domain Reputation ارائه شده توسط افتا ۲. بروزرسانی روزانه آدرس های IP/Domain Reputation بین المللی ۳. بروزرسانی دائمی آدرس IP کشورها ٤. بروزرسانی دائمی ISDB ٥. بروزرسانی دائمی سایت های Phishing ایرانی ٦. بروزرسانی دائمی سایت های Phishing خارجی ۷. بروزرسانی دائمی آدرس اعلام شده بصورت روزانه در سایت افتا ۸. بروزرسانی دائمی سایت ها با دسته بندی های مختلف جهت فیلترینگ ۹. بروزرسانی دائمی آدرس های Ransomware و C&C Srv ۱۰. بروزرسانی دائمی آدرس های Virus، Bot، Spyware ۱۱. بروزرسانی دائمی IDS/IPS ۱۲. بروزرسانی دائمی MAC of NIC manufacturers
2	**مدیریت یکپارچه مرکزی CCM**	قابلیت تعامل با مدیریت یکپارچه مرکزی ۱. امکان اعمال پالیسی های امنیتی فایروال ۲. امکان تعریف Object های مختلف مبتنی بر Network ۳. امکان تعریف زمان بندی های مختلف بصورت Single و Weekly ۴. امکان تعریف Object ها مختلف مبنی بر پروتکل و پورت ۵. امکان کسب انواع گزارشات بصورت تجمیعی و یکپارچه ۶. امکان تعیین دسته بندی ها و گروه بندی های مختلف
3	**بخش فایروال**	۱. کنترل و جلوگیری هوشمند از حملات آنومالی و مشکوک (Mass Security) ۲. تشخیص هوشمند حملات پیشرفته (Smart ATP Security) ۳. قابلیت Traffic Limitation جهت جلوگیری از حملات DoS و DDoS ۴. کنترل و تشخیص نرم افزارها شامل فیلترشکن ها، دانلودرها و ... (Application Awareness) ۵. عملکرد شناسه محور و تشخیص بر حسب شناسه های کاربری و ... (Identity Awareness) ۶. شناسایی و کنترل ماهیت پورت ها (Port Enforcement) ۷. دارای عملکردهای اختصاصی شامل Tarpit جهت ایجاد Loop در درخواست ها و Hijack جهت شبیه سازی درخواست ها و اعمال تغییرات ۸. دیتابیس تشخیص و کنترل آدرس های کمپانی های مشهور (ISDB IP Detection and Protection) ۹. پشتیبانی از پروتکل های پیشرفته SCTP و GTP ۱۰. پشتیبانی از کنترل و مدیریت ترافیک های VOIP (SIP NAT Traversal)

۹ - این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

4	**بخش تنظیمات شبکه**	۱. امکان تعامل و اتصال کامل به سامانه مدیریت مرکزی (CCM) جهت اعمال پالیسی های امنیتی و گزارش گیری های یکپارچه و مجتمع ۲. امکان تعامل و دستور پذیری از سامانه های SIEM و تجهیزات SOC ۳. پشتیبانی کامل از IP نسخه 6 ۴. پشتیبانی از قابلیت Router Advertisement در IP نسخه 6 ۵. پشتیبانی از کانکشن های PPPOE و اعمال کلیه فرایندها و سرویس ها ۶. ارائه خدمات Access Point در سخت افزارهای دارای آنتن WIFI
5	**بخش VPN و سرویس های دورکاری**	۱. پشتیبانی کامل از تانل اختصاصی L3 Kangaroo با عملکردSite to Site ۲. پشتیبانی از ارتباطات اختصاصی L3 و L7 SSL با عملکرد Client to Site ۳. قابلیت DmVPN یا Dialup VPN تحت عنوان L3 VPN اختصاصی ۴. امکان Include و Exclude کردن اختصاصی ترافیک در انواع VPN ۵. امکان مرتبط نمودن ارتباطات VPN با توکن های سخت افزاری ۶. امکان مرتبط نمودن ارتباطات VPN با گواهی نامه های امنیتی
6	**خدمات دسکتاپ مجازی**	۱. امکان احراز هویت کامل و یکپارچه کاربران مجازی بصورت VDI ۲. اکانتینگ و حسابرسی کاربران VDI بصورت شناور ۳. کنترل پهنای باند و مدیریت زمان و حجم کاربران VDI بصورت کاملا شناور ۴. تشخیص و احراز هویت کاربران VDI در کلیه مدل های عملکردی (L3 NAT / L3 Route / Core VLAN) ۵. ثبت لاگ کامل و ارائه گزارش سایت های بازدید شده VDI(حتی SSL و TLS)

7	**آنتی فیشینگ**	۱. امکان تشخیص و جلوگیری از دسترسی به سایت های فیشینگ ایرانی ۲. امکان تشخیص و جلوگیری از دسترسی کاربران به سایت های فیشینگ بین المللی
8	**بخش خدمات فیلترینگ**	۱. فیلترینگ کامل URLوب و سایر پروتکل های لایه کاربرد بر حسب: ○ نوع مرورگر (User Agent) ○ درخواست کاربر (Req Header) ○ پاسخ درخواست ها (Res Header) ○ انواع فایل ها و کدهای اجرایی از جمله JS و Activex و ... ۲. فیلترینگ کامل سایت ها و آدرس های SSL و TLS ۳. ارائه قابلیت URL rewrite redirect جهت هدایت درخواست های وب ۴. فیلترینگ کامل تمامی Mime Type ها ۵. فیلترینگ بر اساس بیش از ۵۵ دسته بندی مختلف
9	**خدمات جلوگیری از نشت اطلاعات (DLP)**	۱. جلوگیری از نشت اطلاعات در Gateway بر اساس نوع فایل ها ۲. جلوگیری از نشت اطلاعات در Gateway بر اساس نام و مشخصات فایل ها ۳. اعمال DLP بصورت شناسه محور بر روی کاربران، گروه ها، آدرس های IP، آدرس های Network، پالیسی ها و ...
10	**قابلیت های سیستمی**	۱. دارای واسط کاربری اختصاصی بصورت نرم افزاری قابل اجرا در ویندوز، لینوکس و مک ۲. کنترل دسترسی مدیران سیستم از سطوح دسترسی مختلف و ریزدانگی ۳. امکان ذخیره کردن و بازیابی اطلاعات از طریق ابر اختصاصی متعلق به هر مشتری ۴. پشتیبانی و اعمال کامل تنظیمات بر اساس تقویم شمسی و میلادی ۵. مدیریت، تولید و کنترل گواهی نامه ها (CA Management) ۶. کنترل سیستم در حالت Green IT جهت مدیریت منابع انرژی و هوای پاک
11	**خدمات جلوگیری از بدافزارها**	۱. امکان جلوگیری از دسترسی به آدرس های خطرساز حاوی: ○ آدرس های SPAM ○ آدرس های بدافزارهای جاسوسی (Spyware) ○ آدرس های انتشار و حاوی ویروس ○ آدرس های مرتبط با باج افزارها و سرورهای C&C ○ آدرس های مرتبط با بات نت ها ○ آدرس های مشکوک به حمله و خطرساز ۲. اعمال بصورت شناسه محور بر روی کاربران، گروه ها، آدرس های IP، آدرس های Network، پالیسی ها و ...
12	**امکانات رفع اشکال**	

- این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

		۱. تشخیص آدرس های IP بر حسب کشور ۲. امکان Whois نمودن آدرس ها Domain ۳. امکان بررسی سایت های فیشینگ ۴. امکان Speed Test و سنجش سرعت اینترنت دستگاه ۵. بررسی سایت ها در خود دستگاه ۶. امکان TCP Dump و Capture نمودن مستقیم بسته های ارتباطی شبکه
13	**خدمات احراز هویت در زیر سیستم Identity**	۱. احراز هویت کاربران بدون نیاز به Agent یا Dialer ۲. امکان احراز هویت سایت های HTTPS ۳. امکان تشخیص ارتباطات SSL ۴. امکان یکپارچگی با سرویس های SSO از جمله Authin.ir ۵. احراز هویت کاربران بر اساس متدهای زیر: ○ مبتنی بر IP کاربر ○ مبتنی بر MAC Address کاربر ○ مبتنی بر VDI ○ حالت Basic ○ حالت Hotspot ○ حالت NTLM ○ حالت SSO
14	**زیرسیستم Balancer**	۱. امکان موازنه بار لینک های اینترنتی بدون محدودیت در تعداد و نوع مدیا ۲. امکان موازنه بار ترافیک ها و سرویس های داخلی بدون محدودیت تعداد ۳. موازنه بار ترافیک های SSL ۴. امکان تشخیص قطع اتصال لینک ها توسط پروتکل ها TCP، DNS و Ping ۵. موازنه بار تانل های L3 Kangaroo ۶. پشتیبانی از ۱۲ الگوریتم مختلف از جمله: ○ Weighted ○ Persistence Client ○ Persistence Server ○ First Available ○ Lowest latency ○ First available ○ Least Load/Packet/Byte ○ Fastest response ○ ...
15	**زیر سیستم ZTNA APP Control**	قابلیت تعامل **زیر سیستمZTNA APP Control** ۱. امکان مدیریت پهنای باند هر نرم افزار بصورت تفکیک شده در سمت سیستم کلاینت ها ۲. ثبت لاگ ارتباطات و سایت های مشاهده شده توسط نرم افزار ها حتی فیلترشکن ها ۳. امکان تعیین عملکرد بصورت لیست سیاه و سفید ۴. عدم توانایی کاربران در پنهان سازی و تغییر نرم افزارها با روش های مختلف

		۵. امکان تشخیص بدون وابستگی به نسخه نرم افزارها
16	**زیرسیستم ZTNA Traffic Manager**	قابلیت تعامل **زیرسیستمZTNA Traffic Manager** ۱. امکان رمزنگاری ارتباطات بین کلایت های شبکه بدون توجه به VLAN بندی ها و بدون استفاده از تانل های VPN (بصورت کاملا Peer to Peer) ۲. پیا سازی Micro Segmentation ۳. امکان تفکیک منطقی ترافیک اینترنت از شبکه داخلی ۴. اعمال پالیسی های امنیتی فایروال بین کاربران داخل شبکه و محدود نمودن دسترسی ها ۵. ثبت و ارائه گزارشات ارتباطات کلاینت ها با یکدیگر

ضوابط و نحوه ارزیابی پیشنهادات:

۱. شرایطالزام شرکت کنندگان

احراز کلیه شرایط مندرج در ذیل برای شرکت در فرآیند الزامی است. بدیهی است در صورت عدم رعایت هر یک از الزامات مقرر، از گشایش پاکات حاوی پیشنهاد قیمت ایشان ممانعت به عمل خواهد آمد.

۱.۱. دارای تاییدیه افتاء محصول دارای اعتبار
۱.۲. دارای تائیدیه افتا شرکت در زمینه نصب و پشتیبانی محصولات فتا
۱.۳. دارای تائیدیه افتا شرکت در زمینه امن سازی و مقاوم سازی سامانه ها، زیرساخت ها و سرویس ها
۱.۴. دارای گواهی شورای عالی انفورماتیک با تاریخ اعتبار در زمینه امنیت فضای تبادل اطلاعات
۱.۵. دارای گواهی ثبت فنی نرم افزار
۱.۶. دارای گواهینامه دانش بنیان در سطح فناور
۱.۷. دارای تاییدیه پدافند غیرعامل

۲. کامل بودن پیشنهادات

تسلط و تجربه در زمینه موضوع استعلام، از الزامات اساسی برای شرکت در این فرآیند می‌باشد. لذا خواهشمند است سوابق اجرایی خود را به همراه پیشنهادات مربوطه ارسال نمایید.

کارفرما نسبت به بررسی پیشنهادات دریافتی اقدام خواهد نمود تا اطمینان حاصل گردد که مجموعه ارائه‌شده کامل بوده و تمامی جزئیات اطلاعات و مدارک خواسته‌شده به نحو مطلوب ارائه گردیده‌اند. همچنین، مدارک می‌بایست به‌طور صحیح و مطابق با الزامات تعیین‌شده امضا و تأیید گردند.

لازم به ذکر است که اسناد و پیشنهادهای ارسالی باید مطابق با چارچوب‌های مشخص‌شده ارائه شوند و در صورت مثبت بودن نتایج بررسی‌ها، موارد بعدی مورد ارزیابی قرار خواهند گرفت.

۳. ارزیابی فنی و تخصصی

پس از انجام کنترل‌های لازم در خصوص موارد فوق، شرکت‌کنندگان تحت ارزیابی فنی و تخصصی قرار خواهند گرفت. در این ارزیابی، تنها شرکت‌هایی مورد تأیید قرار خواهند گرفت که به تشخیص کارفرما، درک صحیحی از موضوع و ابعاد پروژه داشته و با ارائه مدارک و اطلاعات مربوطه، توانمندی خود را از لحاظ فنی، سازمانی و مالی، به‌ویژه در زمینه تأمین نیروی انسانی مورد نیاز پروژه، به اثبات برسانند.

لذا محصول ارائه شده به هیچ وجه نباید برگرفته از محصولات متن باز و رایگان از جمله pfSense، IPTables و سایر توزیع های مرتبط با انها باشد. شرکت ملی پخش فرآورده های نفتی منطقه بوشهر در انتخاب محصول و پیمانکار مورد نظر خودمختار می باشد.

۱۴ - این مستند در طبقه‌بندی محرمانه تولیدشدهو هرگونه نشر، کپی‌برداری، انتقال به غیر و تغییر محتویات آن تنها با اجازه کتبی از شرکت ملی پخش فرآورده های نفتی منطقه بوشهر میسر است.

۴. مدت زمان اجرا و پشتیبانی پروژه

مدت زمان اجرای این پروژه حداکثر یک ماه تعیین گردیده است و خدمات پشتیبانی رایگان به مدت ۱۲ ماه ارائه خواهد شد. اجرای این پروژه، شامل نصب، راه‌اندازی، و پیکربندی کامل دستگاه به همراه آموزش‌های لازم برای پرسنل مرتبط، می‌بایست به‌طور انحصاری توسط کارشناسان متخصص شرکت مجری انجام پذیرد.

مشخصات حداقلی فنی و سخت افزاری مورد نیاز جهت اجرای پروژه

فایروال تجهیزات حفاظت شبکه های رایانه ایNGFW-UTM

Part Number:۲B۵۰HN۸۰۸

Model: TK۵۲۴۰

Max Concurrent Client: ۴/۰۰۰

Max Concurrent Session: ۴۰/۰۰۰

•Online Update

•Offline Update

•Online Reporting

•Offline Reporting

•License: Unlimited

•Sub Scription: ۱year

جهت استفادهHA