paraflow

Изх. 9691 / 14.08.2020г.

ДО:	**АЕЦ КОЗЛОДУЙ ЕАД**
	Г-н Христо Пачев
E-mail:	**commercial@npp.bg**

ИНДИКАТИВНА ОФЕРТА

по пазарна консултация 44126

с предмет „Модернизация на модулите към системата за Интернет комуникация и повишаване на киберсигурността в информационната инфраструктура на "АЕЦ Козлодуй" ЕАД“

1. ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ – ФУНКЦИОНАЛНОСТИ

1.1	Обособяване на зони с различна степен на доверие, като разделя мрежата на отделни сегменти според функционалните им характеристики;
1.2	На база на акредитация от Активната Директория контролира поведението на всеки един потребител при достъпа му до Интернет и вътрешните ресурси.
1.3	Инспекция на трафика и идентификация на приложенията.
1.4	Защита от мрежови атаки чрез система за превенция на атаките (IPS).
1.5	Системата анализира съдържанието за наличие на зловреден код (AntiVirus и AntiSpyware). Прилага се различен анализ на база категория от URLs или група от приложения.
1.6	Системата има възможност за надграждане с допълнителен лиценз, който позволява анализ на Zero Day зловреден код чрез стартиране на файла във защитената среда. Ще се прилага различен анализ на база приложения, група от приложения и типове файлове.
1.7	Филтриране на уеб сайтовете по категории с цел да се ограничи достъпа на потребителите на вътрешни за мрежа до ресурси до опасно съдържание в Интернет.
1.8	Решението предоставя възможност за мултикатегоризация на URL съгласно тип на съдържанието и риск.
1.9	Решението предоставя възможност за идентифициране на ново регистрирани домейни и ограничаване на достъпа до тях.
1.10	Наличие на DLP (Data Loss Prevention) функционалност, като по този начин ще се осъществява идентификация на файлове по име и разширение, изпращани и/или получавани в мрежовия трафик.
1.11	Инспекция на HTTPS и HTTP 2.0 протокола - декриптиране и инспекция на входяща и изходящ SSL мрежова комуникация.
1.12	Декриптиране на SSL мрежова комуникация, която транспортира в себе си криптирани SMTP, IMAP, POP3, FTP.

paraflow

1.13 Декриптирането на SSL трафика, прозрачно за всички функционални компоненти на системата: IPS, AntiVirus, AntiSpyware, инспекция на данни и файлове, и URL филтриране.

1.14 Политиката за декриптиране има възможност да се настройва на база на URL категория.

1.15 Политиката за декриптиране има възможност да блокира достъпа до даден Web Site в случай, че отсрещната страна не използва необходимо ниво на криптиране или валиден сертификат.

1.16 Системата предоставя възможност за надграждане с допълнителен лиценз, който позволява отдалечен VPN достъп от мобилни устройства (iOS, Android) и Clientless SSL VPN. Включително инспекция (compliance check) на крайно клиентската машина преди изграждането на отдалечен достъп.

1.17 Блокиране на всички приложения, които не са изрично указани като разрешени за използване в конфигурираните в системата политики, да бъдат блокирани.

1.18 Идентификация на приложенията без оглед на използвания от тях комуникационен порт и протокол.

1.19 Възможност за конфигурация на политиките за сигурност чрез дефиниране на източника на мрежовата комуникация, крайната цел на мрежовата комуникация (посока), приложението и/или приложенията, за които се отнася политиката, дефиниране на мрежовите услуги както и каква да бъде активната реакция ако критериите бъдат изпълнени.

1.20 Препращане на подозрителните DNS заявки към специално подбран произволен адрес с цел бърза идентификация и блокиране на комуникацията на заразени хостове от вътрешната мрежа (DNS sinkholing).

1.21 Възможност за дефиниране на VLAN-и за Layer 2 и Layer 3 интерфейсите с цел да се осигурят гъвкави механизми за инспекция на трафика, които да поддържат създадените за нуждите на организацията мрежови сегменти.

1.22 Възможност за изграждане на site-to-site VPN тунели на база IPSec и IKE стандартите.

1.23 Възможност за управление и приоритизиране на трафика (QoS) според типа приложение.

1.24 Прозрачна идентификация на потребителите без изискване да се предоставят потребителско име и парола.

1.25 Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване във външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).

1.26 Възможност за дефиниране на индивидуални маршрутизиращи таблици с цел осигуряване на маршрутизиращи функционалности за различните мрежови сегменти.

1.27 Възможност за конфигурация устройства да работят в режим на отказоустойчивост (High-availability), чрез конфигуриране Active-Active или Active-Passive.

1.28 Възможност за мониторинг, анализ на логовете и репортинг от самото устройство.

1.29 Уеб базиран интерфейс за управление на устройството и индивидуално дефинируеми в системата полета за показване на различни статистики на база време, приложение, категории, потребители и заплахи.

1.30 Логовете на устройството ще са достъпни в уеб интерфейса с възможност за контекстуално филтриране или филтриране на база ключова дума. Информацията ще бъде обогатена контекстуално с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и др.).

1.31 Възможност за интеграция с облачна услуга на същия производител за анализ и отчет на текущите атаки/заплахи както за организацията така и за сходни с нея. Показване на тенденции, анализи и методи за превенция в световен мащаб.

1.32 Решението инспектира DNS трафика на организацията и реализира превенция на атаки базирани на DNS Tunneling.

1.33 Решението разполага с механизъм за следене и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA)).

1.34 Предложените устройства имат възможност за интеграция с решение за SD-WAN от същия

или друг производител.

2. ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ – ПАРАМЕТРИ

2.1	Пропускателна способност с активирана функция за идентификация на приложенията	18 Gbps
2.2	Пропускателна способност с активирани функционалности за IPS/AntiVirus/ AntiMalware защита, URL филтриране и идентификация на файлове и чувствително съдържание в трафика	8.8 Gbps
2.3	Брой TCP сесии	3 800 000
2.4	Брой нови сесии в секунда	132 000
2.5	Брой на разпознати и поддържани приложения	3 183
2.6	Брой интерфейси	4 x 1000 / 10000 Base-T ports Възможност за надграждане допълнителни минимум 16 x 10Gbit/s SFP+ 4 x 40Gbit/s QSFP
2.7	Режими на интерфейсите	L2, L3, Tap, Transparent mode
2.8	Маршрутизиращи функции	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 Bidirectional Forwarding Detection (BFD)
2.9	Изисквания към IPSec имплементация	Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
2.10	Брой конкурентни SSL VPN потребителя включени в системата	10 000 SSL VPN потребителя
2.11	Брой IPSec Site-to-Site VPN	3000 отдалечени точки
2.12	Устройството поддържа виртуални контексти	10 броя
2.13	Устройството поддържа виртуални таблици за маршрутизация минимум	20 броя
2.14	Брой поддържани VLAN	4,094 броя IEEE 802.1q VLAN маркера (tags), конфигурируеми за всеки интерфейс и общо за устройството
2.15	IPv6 поддръжка	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
2.16	Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за	Системата декриптира и инспектира SSL

	инспекция и налагане на политики над съдържанието	
2.17	Управление на канала	Управлението на канала (QoS) е налично и приложимо за всяко идентифицирано приложение
2.18	Управление на устройството	Всяко от устройствата в системата има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
2.19	Режим на надеждност	Active/Active, Active/Passive
2.20	Брой интерфейси за управление	1 x 10/100/1000 out-of-band management port 1 x 40 Gbit/s интерфейси за отказоустойчивост 1 x RJ-45 конзолен порт
2.21	Монтаж и размери	Предназначена за вграждане в 19'' шкаф с размер 3U
2.22	Захранване и входно напрежение (Входяща честота)	Резервирано, 100-240VAC (50-60Hz)
2.23	Софтуерна и хардуерна гаранционна поддръжка 365x24x7	36 месеца с партиден номер от Производителя

paraflow

3. ЦЕНОВА ОФЕРТА

	Описание			Ед. Цена в лв без ДДС	Стойност в лв без ДДС
1.	Palo Alto Networks PAN-PA-5220 в клъстер, с описаната по горе функционалност и параметри	бр.	2	249 980.00	499 960.00
				Обща стойност без ДДС	**499 960.00**

Наименование	"ПАРАФЛОУ КОМУНИКЕЙШЪНС" ООД
ЕИК	831913775
Адрес	Гр. София 1700, ул. „Никола Габровски" №79
E-mail	office@paraflow.bg
Телефон	00359 2 9604200
Лице за контакт	Димитър Цонев
Длъжност	Мениджър продажби

Срок за изпълнение – до 90 календарни дни.

Условия на доставка – до складовете на АЕЦ Козлодуй.

Съпроводителна документация при доставката – съгласно изискванията в Техническото задание.

Заличено на основание ЗЗЛД

С уважение: .....

Д

М

„Парафлоу Комуникейшънс" ООД

На вниманието на:
АЕЦ Козлодуй ЕАД

Уважаеми,

КЛИКО България ЕООД в качеството си на оторизиран дистрибутор за продуктите на Palo Alto Networks за територията на България, потвърждава, че **Парафлоу Комуникейшънс ООД**, с ЕИК 831913775 и седалище в гр. София, бул. Никола Габровски 79 е оторизиран партньор на Palo Alto Networks и е упълномощен да продава оборудване и гаранционна поддръжка на територията на Република България. **Парафлоу Комуникейшънс ООД** е акредитиран партньор на Palo Alto Networks с ниво „Innovator".

Парафлоу Комуникейшънс ООД не е упълномощен да се съгласява с каквито и да е общи условия от името на Palo Alto Networks и КЛИКО България ЕООД и никакви условия не бива да се прилагат или да са приложими за Palo Alto Networks и КЛИКО България. Всички продукти се продават при спазване на условията на лиценз за краен потребител на Palo Alto Networks и споразумение за ограничена гаранция.

Заличено на основание ЗЗЛД

11.08.2020 год.
София

С уважение,
Александър Стаменов
Управител
Клико България ЕООД