



FO-08-01-04

Nr. 31221 / AJOFM/II.D.16 / 10.12.2019

ANUNT-ACHIZITIE DIRECTA

Agenția Județeană pentru Ocuparea Forței de Muncă -Prahova, cu sediul în Ploiesti, str. Nicolae Iorga, nr.1, județ Prahova, telefon: 0244/571380, intenționează să achiziționeze prin achiziție directă, "ROUTER CU CAPACITATE DE CRIPTARE", în conformitate cu prevederile art. 7 alin. 5 din Legea nr. 98/2016 privind achizițiile publice cod CPV 32420000-3- *Echipament de retea* .

Obiectul contractului: Achiziționare ROUTER CU CAPACITATE DE CRIPTARE conform cerințelor din caietul de sarcini, disponibil pe site-ul Agenției Județene pentru Ocuparea Forței de Muncă -Prahova secțiunea Anunțuri <http://www.anofm.ro/>

Cantitatea - Se vor achiziționa 6 buc routere cu capacitate de criptare.

Valoarea totală estimată a contractului: Valoarea estimată este de de 25.000 lei fără TVA

Criteriul de atribuire -Pretul cel mai scazut

Conditii de participare: Achizitia directa se va face direct din platforma SICAP si va fi finalizata prin incheierea unui contract de furnizare de produse .

Ofertantii interesati pot trimite oferta LA SEDIUL ajofm Prahova str. Nicolae Iorga nr. 1 et.1 sau pe e-mail gabriela.spasici@ph.anofm.ro pana la data de 16.12.2019 ora 10.00

Oferta trebuie sa respecte specificatiile tehnice anexate prezentului anunt si sa se incadreze in bugetul estimat .



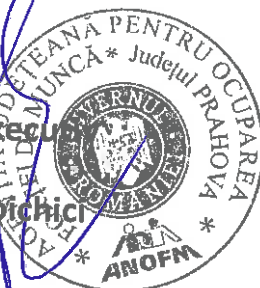
MINISTERUL MUNCII
ȘI PROTECȚIEI SOCIALE



Pentru informatii suplimentare operatorii economici interesati se pot adresa la sediul
agentiei, tel: 0244/571333, 0725.786221 fax: 0244/571333, sau e-mail
gabriela.spasici@ph.anofm.ro

Director Executiv

Cristina Stoichici



Director Executiv Adj

Roxana Valentina Vilau

Intocmit,

Compartiment Achizitii Publice

Gabriela Spasici



SPECIFICAȚII TEHNICE ECHIPAMENT

Caracteristici generale	Echipamentul va trebui să se integreze în arhitectura de comunicații actuală. Echipamentul va putea să fie montat într-un rack, ocupând 1RU dimensiune
Hardware	Echipamentul va include kit de montare în rack.
Șasiu	2 porturi Ethernet de WAN din care minim 1 port Gigabit, cu personalitate duală RJ-45 / SFP. Echipamentul trebuie să fie prevăzut cu cel puțin 8 porturi LAN Gigabit, din care minim 4 porturi capabile PoE. Memorie RAM: minim 512 MB Memorie flash: minim 256MB Porturi USB 2.0: minim 2
Arhitectură și Performanță	Echipamentul va oferi posibilitatea managementului out-of-band folosind un port de consola RJ-45 . Porturile USB onboard vor oferi posibilitatea de atașare a unei memorii flash suplimentare. Min. 14 VLAN-uri 802.1q suportate. Accelerator hardware pentru funcțiile de criptare
Securitate	Firewall: - Echipamentul va oferi implementarea unui firewall de tip stateful, cu suport pentru VRF-uri. - Echipamentul va oferi posibilitatea implementării unui firewall bazat pe zone de securitate. - Suport pentru funcționalități de tip IPS și Content Filtering Criptare: - DES, 3DES, AES-128, AES-256 VPN: - Accelerare IPSEC hardware



	- Suport DMVPN pentru integrarea în arhitectura curentă. - Număr de tunele IPSEC suportate: minim 50 - SSL VPN
Management	Interfața de management completă în linie de comandă (CLI) Echipamentul va putea fi administrat de la distanță prin Telnet, SSH, HTTP Echipamentul va trebui să poată fi integrat într-o aplicație de management de rețea pentru operațiunile de management (configurare, monitorizare), care va fi inclusă în ofertă. Sistemul de management trebuie să conțină toate componentele software și licențele necesare pentru asigurarea monitorizării tuturor echipamentelor de tip router din cadrul proiectului. Pentru autentificarea utilizatorilor ce administrează echipamentele, acesta se va integra nativ cu o soluție centralizată de management a politicilor de acces în infrastructura de rețea, care va fi inclusă în ofertă. Aplicația va implementa funcția de server TACACS+ pentru administrarea accesului auditat către infrastructură. Sistemul centralizat de management al politicilor de acces în infrastructura de rețea trebuie să permită pe viitor adăugarea de funcționalități precum: autentificarea și autorizarea utilizatorilor care se conectează la rețea prin conexiune pe fir, wireless sau VPN, va permite urmărirea în mod curent și în istoric a fiecărui utilizator și device și a activității acestuia din punct de vedere autentificare și autorizare, identificarea echipamentelor de pe care se conectează și aplicarea de politici de securitate respectivelor device-uri, realizarea unui audit al dispozitivelor ce încearcă să se conecteze și să verifice dacă acestea îndeplinesc criteriile prestabilite de securitate și stabilitate necesare funcționării în cadrul instituției, înainte ca acestea să aibă acces în rețea; În cazul în care dispozitivele nu îndeplinesc criteriile prestabilite de securitate, aplicația va lua măsuri de carantina și de izolare până când dispozitivele se remediază.
Sistemul de management	Sistemul de management trebuie să poată oferi rapoarte de tip End-of-Sale/End-of-Life pentru echipamentele din rețea. Sistemul de management trebuie să asigure cel puțin următoarele funcții principale:



- monitorizarea alarmelor echipamentelor de rețea, managementul configurațiilor echipamentelor, managementul update-urilor sistemelor de operare ale echipamentelor, inventarierea echipamentelor (tip, componente, serii, etc.), managementul performanței echipamentelor, capabilități de raportare.
- Sistemul de management trebuie să poată fi accesibil printr-o interfață Web, HTML5, ce permite operarea facilă de pe PC sau tabletă.
- Sistemul de management trebuie să se poată integra cu LDAP/AD pentru autentificarea utilizatorilor, permițând accesul pe baza de roluri pentru asigurarea de privilegii diferite pentru categorii diferite de utilizatori.
- Sistemul de management trebuie să ofere simplificarea implementării unor noi echipamente și site-uri, suportând funcționalități de tip plug-and-play pentru configurarea automată a echipamentelor noi.

Sistemul de management trebuie să asigure monitorizarea echipamentelor, oferind cel puțin următoarele facilități:

- sistem centralizat de colectare log-uri (syslog) cu facilități de filtrare
- suport pentru colectare SNMP-traps și configurarea de alerte pentru trap-urile primite
- listarea evenimentelor din rețea și generarea alarmelor
- posibilitatea de a seta praguri pentru alertele de performanță (ex: încărcare CPU, încărcare interfață, etc.)
- severități diferite pentru alarme
- Sistemul de management trebuie să ofere fluxuri de lucru (workflow) integrate pentru a facilita descoperirea întreruperilor de serviciu, degradarea performanței prin notificări și implementarea acțiunilor de remediere.

Sistemul de management trebuie să asigure managementul configurațiilor și al software-ului echipamentelor, oferind cel puțin următoarele facilități:

- template-uri predefinite de configurare automată a anumitor funcționalități pe echipamente(ex: ACLs, AVC, firewall zone-based, VPN, etc.)



- arhivarea configurațiilor, cu posibilitatea reținerii mai multor versiuni pentru același echipament
- aplicarea unei configurații sau a unui subset de comenzi pe mai multe echipamente simultan
- update-ul sistemului de operare de pe echipamente
- verificarea conformității configurațiilor echipamentelor prin definirea unui template parametrizabil și auditarea echipamentelor din rețea pe baza acestui template, cu posibilitate de remediere automată a configurațiilor.

Sistemul de management trebuie să asigure managementul performanței oferind cel puțin următoarele facilități:

- monitorizarea parametrilor de încărcare standard (CPU, Memorie, utilizare interfețe, etc.)
- elemente și template-uri pentru simplificarea configurației elementelor integrate de instrumentare a performanței (de exemplu AVC, Netflow, NBAR2), pentru configurarea automată a echipamentelor de rețea și reducerea complexității colectării datelor
- Sistemul de management trebuie să ofere suport pentru monitorizare netflow, pentru a furniza detalii referitoare la consumul de bandă, aplicațiile folosite și cantitatea de bandă consumată per aplicație.
- Sistemul de management trebuie să ofere monitorizarea furnizând informații despre politicile QoS definite și aplicate pe interfețe și modele de trafic existente, precum și monitorizarea aplicațiilor de voce și video în rețea pentru a facilita diagnosticarea echipamentelor

Sistemul de management trebuie să ofere capabilități extinse de raportare pentru datele colectate oferind cel puțin următoarele facilități:

- șabloane predefinite de rapoarte, incluzând rapoarte de resurse și inventar, rapoarte de analiză, rapoarte de tip trend, top-N și rapoarte pentru defecte
- crearea, modificare, ștergere, vizualizare online, exportare și generare periodică a rapoartelor
- posibilități de personalizare a rapoartelor, inclusiv gruparea mai multor rapoarte în unul singur



	Sistemul de management trebuie să includă funcționalități ce permit în viitor managementul unei rețele wireless, incluzând cel puțin următoarele facilități: - Elemente pentru planificare și design de rețele wireless (inclusiv importare hărți și plasarea access-point-urile pe hartă), - vizibilitatea și managementul elementelor RF, - determinarea și urmărirea locației utilizatorului, - sistem de wireless intrusion prevention și configurații ale rețelei wireless, LAN, monitorizare și management
Funcționalități de rutare	Sistemul de operare al echipamentului va include suport pentru următoarele protocoale și funcționalități (inclusiv licențele aferente, dacă este cazul): - IPv4, IPv6 - RIP v1 și v2 - Bidirectional Forward Detection (BFD) - Open Shortest Path First (OSPF) - Enhanced IGRP (EIGRP) - Border Gateway Protocol (BGP) - NAT - Policy-Based Routing (PBR) for Traffic Management - IP sec - Layer 2 Tunneling Protocol Version 3 (L2TPv3) - Bidirectional Forwarding Detection (BFD) - VRF Lite - DMVPN - IPSec VPN - QoS, Class-Based Weighted Fair Queuing (CBWFQ), Class-Based Weighted Random Early Detection (CBWRED), Hierarchical QoS
Garanție	Garanție hardware minim 3 ani, asigurată de producător. Ofertantul va prezenta, în orice formă, dovada asumării garanției de către producător



	pe perioada solicitată. Acces la upgrade-uri software de pe pagina de internet a producătorului pe perioada garanției. Ofertantul va prezenta, în orice formă, dovada faptului că echipamentele livrate beneficiază de acces la upgrade-uri software din partea producătorului. Access la suportul tehnic al producătorului prin telefon, e-mail, caz electronic pe perioada garanției. În perioada de garanție, toate operațiunile de înlocuire ale componentelor hardware vor fi efectuate de către ofertant.
Disponibilitate	Produsele oferite trebuie să fie noi și să nu trebuie să fie End of Life sau End of Sales la data depunerii ofertei. Ofertantul va prezenta dovada faptului că echipamentele oferite sunt noi și nu sunt End of Life sau End of Sales la data depunerii ofertei.