NR. 151056 / 13.11.2024

Specificaţii tehnice minimale

"Soluţie securitate acces reţea de tip NAC"

Descriere generala	Soluție de control a accesului in rețea cu fir, fara fir si VPN, pentru dispozitive si utilizatori ce oferă vizibilitate, control și raspuns automat la incidente.
Mod de operare	Soluția trebuie să se implementeze centralizat, într-o arhitectură de tip out-of-band (nu trebuie sa stea in-line cu traficul). Soluția sa ofere, de asemenea, managementul utilizatorilor de tip Guest si Contractori cu mai multe portaluri captive personalizabile și conformitatea dispozitivelor
	Soluția nu trebuie sa fie restricționata de utilizarea 802.1x pentru a oferi control al accesului. Poate folosi diferite alte metode pentru a impune controlul: SNMP, CLI/SSH, API, Syslog in functie de producatorul de echipamente de retea cu care se integreaza.
Tip Appliance	Mașină virtuală (VMWare/Hyper-V/AWS/Azure/KVM)
Performanţă	Suporta 5.000 porturi de rețea, dar este scalabil până la 15.000 de porturi de rețea prin adăugarea de resurse fizice la server (vCPU, RAM)
Suport dispozitive	Este licențiat pentru controlul a 500 dispozitive cu posibilitate de extindere.
Arhitectură	Arhitectura centralizată, în care serverul NAC este plasat într-o locație centrală (nu in-line), dar poate controla dispozitive din alte locații fără a utiliza sub-componente de analiza trafic in acestea
	Managementul serverului de aplicare a politicilor și al portalului invitat/captiv în același appliance.
Integrare cu alte componente din reţea	Dispozitive de infrastructură de rețea (cu fir și fără fir) de la diferiți furnizori
	Dispozitive de infrastructură de securitate de la diferiți furnizori (Firewall, IPS, Sandboxing)
	Servicii de autentificare: RADIUS de la diferiți furnizori
	Servicii de director: LDAP, Microsoft AD, Google SSO

	Sisteme de operare: MAC OS, Microsoft Windows, Linux, Apple IOS, Android
	Securitate pentru endpointuri (AntiVirus), diferiți furnizori acceptați.
	Mai mulți furnizori MDM (AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, FortiClient EMS) utilizati pentru înregistrarea rapida a unui dispozitiv intern
	Soluție este potrivita pentru înregistrarea statiilor de lucru interne, a dispozitivelor de tip Guest precum si a dispozitivelor de tip IoT (ce nu dispun de suplicant EAP) utilizând si alte metode in afara MAB (Mac Authentication Bypass)
Integrare cu echipamente de infrastructura existente in reteaua beneficiarului	- Echipamentele existente in infrastructura actuala sunt: Fortigate 1100E; FortiWeb1000E; FortiAnalyzer VM64, FortiClient EMS. - pentru a primi incidente de securitate (loguri) a.i. solutia de NAC sa ia decizii automate in funcție de gradul de severitate (carantinare la nivel de port de switch sau ssid, dezactivare port switch, notificare Administratori) - schimb de etichete (tag-uri) a.i. Fortigate sa le utilizeze in cazul autentificărilor de SSO pe politici de securitate - primește sesiuni de la acesta pentru a sprijini in identificarea corecta a dispozitivelor
	Soluție Wi-Fi Fortinet bazata pe Controllerul Wireless integrat in echipamentul existent Fortigate: controlează dispozitivele conectate la rețeaua Wi-Fi bazata pe controller wireless Fortigate si FortiAP-uri
	Soluția NAC trebuie să permită definirea graduală a accesului la diferite resurse de rețea protejate, bazate pe regulile definite de compliantă a stațiilor ce se vor conecta la diferite concentratoare de VPN(Cisco, Fortinet, etc.)
	Soluție Switching bazată pe echipamente Fortinet si Cisco (seria C2960; 3650; ISR4451) pentru a controla dispozitivele conectate la acestea in rețeaua beneficiarului
	FortiAnalyzer: pentru a genera rapoarte specifice soluției de NAC
Caracteristici	Oferă capacitatea de a valorifica identitatea utilizatorului, tipul de dispozitiv și combinația celor două pentru a furniza în mod dinamic accesul bazat pe roluri - diferite niveluri de acces
	Crearea un inventar în timp real al tuturor dispozitivelor din rețea si publicarea lor intr-un panou

	Include multiple facilitați de identificare a dispozitivelor inclusiv pentru cele IoT si interoghează serverele producătorului pentru a obține o identificare mai precisa (un scor mai bun)
	Oferă administrarea utilizatorilor de tip Guest si Contractori cu mai multe portaluri captive personalizabile și conformitatea dispozitivelor
	Soluția pune la dispoziție un flux pentru BYOD (stații si alte dispozitive)
	Evaluarea riscului dispozitivelor prin validarea conformității cu diferite criterii: tipul si versiunea sistemelor de operare, existenta soluțiilor de protecție client (eg AV), procese, servicii, etc...
	Oferă funcționalități bazate pe roluri de Administratori . Soluția trebuie să ofere capacitatea de a limita și controla nivelul de acces pe care o oferă soluția diferitelor grupuri administrative din cadrul organizației IT. De exemplu. – Operațiuni de securitate, operațiuni de rețea, help-desk.
	Conectarea funcționalităților NoC-SoC, integrarea evenimentelor de securitate în platformă și reacționarea automată cu dispozitivele vulnerabile la nivelul de acces la rețea și notificarea echipei SOC
	Soluția trebuie să ofere o pistă de audit completă a tuturor conexiunilor la rețea – atât cu fir, cât și fără fir. Aceasta trebuie să includă o interfață ușor de utilizat pentru a căuta și a interoga aceste date.
	Soluția trebuie să includă opțiuni flexibile de scanare atât pentru platformele Windows, cât și pentru OS X si Linux utilizând agenți cu ambele opțiuni Agent instalabil și Agent dizolvabil
	Soluția ar trebui să identifice și să clasifice fiecare tip de dispozitiv din rețea, să identifice dacă este emis de companie sau deținut de angajați și să identifice utilizatorul de pe dispozitiv pentru a activa politicile de acces la rețea bazate pe roluri. Metodele de profilare nu trebuie să necesite vizibilitatea traficului de rețea
	Soluția trebuie să simplifice integrarea dispozitivului prin eficientizarea procesului de înregistrare. Flexibilitatea de integrare a oaspeților ar trebui să includă delegarea către sponsorii invitați, precum și opțiunea pentru oaspeți de a-și înregistra propriile dispozitive - transferând volumul de lucru de la IT la utilizatorii finali

	Soluția trebuie să permită integrarea dispozitivelor personale la o conexiune wireless sigură. Configurarea automată a SSID-ului securizat ar trebui să fie acceptată pentru platformele Windows, Mac, iOS și Android
	Utilizează mai multe metode de profilare (scanare activă și pasivă, amprentă DHCP, SNMP, SSH, scanare TCP/UDP, OUI Producător, agent, IP range, WinRM, Radius, locație de conectare, HTTP/S) pentru a identifica și profila un dispozitiv
	Soluția include Agent care poate fi instalat pe stațiile interne pentru a furniza informații despre acestea dar si pentru a fi utilizat in procesul de înregistrare sau complianța
	Asigura răspuns automat la incidente de securitate primite de echipamente specifice (FW, IPS) si generează evenimente de securitate cu acțiuni asociate: trimite către o soluție SIEM informații contextuale extinse, carantinează dispozitivul la nivel de ssid sau switch, dezactivează port, informează administratori de rețea
Management	GUI HTTPS
	CLI
Disponibilitate	Suportă arhitectura activ-pasivă (atât rețelele de nivel 2, cât și de stratul 3)
Suport	3 ani, 24 x 7, atât licențele pentru dispozitivul server, cât și pentru dispozitivele licențiate.
	Include suport tehnic și upgrade-uri de firmware
Instalare si configurare	Furnizorul va asigura instalarea, configurarea, integrarea si punerea in funcțiune a soluției pana cel tarziu in data de 13 decembrie 2024, conform cerințelor beneficiarului. Furnizorul va asigura instruirea personalului desemnat din partea beneficiarului pentru utilizarea soluției livrate. Serviciile vor include dar nu se vor limita la: configurări, modificări de politici, răspuns si rezolvări de incidente si actualizări.