CAIET DE SARCINI

SISTEM DE SECURIZARE A CONEXIUNILOR METROPOLITANE SI NATIONALE IPSEC

1. Echipament integrat de protectie a retelei ce functioneaza ca o solutie de securitate unificata - 1 buc.

Specificatii	**Cerinte tehnice minimale**
Specificatii hardware	• Interfete GbE RJ-45: 12 • Interfete management/HA/DMZ GbE RJ-45: 1/2/1 • Interfe WAN GbE RJ45: 2 • Interfete 10GbE SFP+Sloturi: 2 • Interfete GbE RJ45/SFP Shared Ports: 4 • Sloturi GbE SFP: 4 • Porturi consola RJ-45: 1 • Porturi USB: 1 • Dimensiune: 1U
Caracteristici	• Trafic firewall (1518/512/64 byte pachete UDP): 20/18/10 Gbps • Latenta Firewall: 5 µs • Trafic Firewall masurat in pachete per secunda: 15 Mpps • Trafic IPSec VPN: 11.5 Gbps • Trafic IPS : 2.5 Gbps • Trafic NGFW: 1.5 Gbps • Performanta SSL Inspection (IPS, HTTPS): 1 Gbps • Numar de tunele IPSec VPN site-to-site: 2.500 • Numar de clienti IPSec VPN: 15.000 • Trafic SSL-VPN: 750 Mbps • Numar de clienti concurenti SSL-VPN: 500 • Numar de sesiuni concurente TCP: 1.500.000 • Numar de sesiuni noi pe secunda TCP: 55.000 • Numar de politici de securitate: 10.000 • Numar de instante virtuale: 10 • Numar de AP-uri administrate: 64 • Trafic CAPWAP (HTTP 64K): 15 Gbps • Numar de token-uri OTP administrate: 5.000 • Numar minim de clienti endpoint administrati: 600

Functionalitati generale	• Echipament integrat de securitate cu functionalitati simultane de:
	  • Firewall de tip stateful
	  • Router cu suport pentru protocoale de rutare dinamice
	  • Posibilitate de instalare in mod bridge Ethernet
	  • Protectie Antivirus
	  • Criptare de date: IPSec VPN si SSL VPN
	  • Suport pentru QoS si Traffic Shaping

	• Detectia si prevenirea intruziunilor – IDS/IPS • Scanare si filtrare WEB – Web Inspection/Filter • Blocarea si controlul traficului din retea generat de aplicatii • Protectie Antispam • Protectie impotriva scurgerii de informatii confidentiale • Update-uri automate si in timp real • Suport pentru IPv6 UTM • Functionalitate de proxy SSL – posibilitatea inspectiei traficului criptat • Wireless controller ● Toate functionalitatile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum si platforma hardware apartin aceluiasi producator ● Certificari pentru producator si produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS, Antivirus ● Conformitate cu: CE, CB
Functionalitati securitate	
Functionalitati firewall	● Functionalitati NAT, PAT si Transparent Bridge ● Optiune de a aplica NAT per politica ● Suport VLAN Tagging 802.1Q ● Autentificarea utilizatorilor pe grupuri ● Suport VoIP SIP/H.323/SCCP Traversal NAT ● Functionalitate proxy explicit HTTP/HTTPS si FTP ● Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru functionalitatea proxy explicit ● Suport WINS ● Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing) ● Suport pentru TCP MSS clamping ● Suport pentru rescrierea campului Class of Service ● Suport IPv6 (NAT/mod Transparent) ● Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de statie folosit – functionalitate de tip BYOD (bring your own device) ● Optiune “Scheduling” pentru politicile de firewall ● Posibilitate de blocare a traficului dupa tara de origine a sursei sau destinatiei (Geo IP)
Functionalitati VPN	● Suport PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN ● Criptare DES, 3DES, AES 128, AES 192, AES 256 ● Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512 ● Suport pentru PPTP si L2TP VPN Client Pass Through ● Functionalitate “Hub and Spoke” IPSec VPN ● Autentificare IKE prin certificate X.509 - suport pentru RSA si ECDSA ● Suport IPSec Xauth NAT Traversal ● Suport configurare IPSec automata ● Functionalitate IKE Dead Peer Detection ● Suport pentru RSA SecureID ● Suport Single-Sign-On pentru pentru book-mark-uri portal SSL-VPN

	• Functionalitate Two-Factor Authentication pentru SSL-VPN • Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) • Suport tunele SSL in mod tunel si in mod portal • Suport pentru validarea clientilor SSL VPN prin verificarea aplicatiilor instalate pe statie inainte de conectare - comaptibilitate cu sistemele de operare Windows • Suport pentru autentificarea utilizatorilor de tip Single Sign On prin portalul SSL VPN • Functionalitati monitorizare tunele VPN • Producatorul are in portofoliu client de VPN IPSec si SSL propriu, care are si functionalitati de: antivirus, filtrare web si optimizare de banda, filtrare a traficului de aplicatii, scanare de vulnerabilitati
Functionalitati Antivirus	• Protectie anti-malware (virus, troian, worm, spyware, grayware) • Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, MAPI, FTP • Suport scanare antivirus Proxy-Based si Flow-Based • Suport pentru detectia malware prin sandboxing de tip Cloud-Based al fisierelor suspecte, prin achizitia unei licente suplimentare • Suport pentru carantina a fisierelor infectate • Protectie impotriva retelelor botnet si site-urilor de tip phishing pe baza de reputatie a adreselor IP si a URL-urilor accesate de utilizatori
Functionalitati filtrare trafic WEB	• Filtrare pentru protocoalele HTTP si HTTPS • Blocare a conexiunilor in functie de URL/cuvant cheie sau expresie in continutul paginilor web • Blocare a conexiunilor in functie de URL-ul din header-ul Referer al cererii HTTP • Filtrare pentru Java Applet, Cookies, scripturi Active X • Posibilitate de activare fortata a optiunii „Safe Search” pentru motoare de cautare web • Posibilitatea de modificare a header-elor HTTP din cererile generate de utilizatori • Functionalitate de monitorizare a activitatii web a utilizatorilor • Posibilitate de instiintare a utilizatorilor, prin afisarea informatiilor in cadrul unui browser web, privind paginile web blocate
Functionalitati sistem de control al aplicatiilor	• Identificarea si controlul a peste 2500 de aplicatii • Optiune de Traffic-Shaping per aplicatie • Clasificare granulara a aplicatiilor dupa criterii multiple precum: Categorii de aplicatii, Popularitate, Tehnologie si Risc • Monitorizare aplicatiilor cu rata cea mai mare de consum de banda • Monitorizarea aplicatiilor pe baza IP/Utilizator • Suport pentru decriptarea si inspectarea sesiunilor SSH • Suport pentru blocarea aplicatiilor utilizate in cadrul retelelor de tip Botnet • Posibilitate de definire a semnaturilor de aplicatie personalizate • Posibilitate de instiintare a utilizatorilor, prin afisarea informatiilor in cadrul unui browser web, privind traficul de aplicatii blocat
Functionalitati sistem de prevenire a intruziunilor/atacurilor (IPS)	• Protectie pentru peste 10000 de semnaturi de atac • Suport pentru inspectia traficului de aplicatie criptat prin protocolul SSL • Protectie pentru atacuri de tip brute force

	• Detectarea anomaliilor de protocol • Suport pentru semnaturi configurabile • Update-uri automate pentru semnaturi • Suport pentru IPv4 si IPv6 DDoS
Functionalitati Antispam	• Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS • Suport RBL/ORDBL • Filtrare dupa cuvinte cheie/expresie • Filtrare dupa Black/White List pentru adrese IP si e-mail
Functionalitate Data Leak Prevention	• Blocare dupa tip si dimensiune fisier

Functionalitati sistem de verificare a statiilor (Endpoint Control)	• Integrare cu o aplicatie software pentru securitate ce ruleaza pe statii care sa permita:
	  • Blocarea traficului de aplicatii instalate pe statii
	  • Restrictionarea/filtrarea accesului web
	  • Scanare Antivirus

Functionalitati retea	
Functionalitati retelistica si rutare	• SD-WAN-control inteligent al interfetei WAN, prin directionarea traficului prin aceasta având link-uri configurate care pot sustine peste 3000 de aplicații și utilizatori/grupuri de utilizatori. Suport pentru legaturi WAN multiple cu balansare a traficului dupa metodele: Weighted round robin a sesiunilor, impartire proportinala a volumului de trafic, prin limitarea per interfata a benzii maxime utilizabile, dupa calitatea conexiunii ISP (jitter sau latenta). • Suport PPPoE si DHCP Client/Server • Rute statice • Rutare dinamica IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS • Rutare dinamica IPv6: RIPng, OSPF v3, BGP 4+ • Gruparea interfetelor in zone de securitate • Policy-based routing • Suport VRRP si Link Failure Control • Suport VLAN Tagging (802.1q) • Suport pentru IPv6 (Firewall, DNS, SIP) • Suport One-to-One NAT • Suport NAT64, DNS64, NAT46, NAT66 • Suport LLDP

Functionalitate Wireless Controller	• Modul wireless controller pentru thin-AP-uri integrat cu urmatoarele functionalitati:
	  • Detectie si suprimare a AP-urilor neinregistrate in controller;
	  • Selectie automata a canalului pentru AP in functie de interferentele din mediu;
	  • Suport pentru SSID-uri multiple;
	  • Autentificare WEP, WPA, WPA2, WPA2 Enterprise, 802.1x
	  • Suport Captive Portal;
	  • Suport pentru Wireless Mesh si roaming;
	  • Distribuire automata a clientilor wireless per AP sau banda de frecvente pentru a obtine performante optime.

	• Rutare dinamica a traficului generat de utilizatorii wireless prin VLAN-uri folosind autentificare prin RADIUS • Autentificare suplimentara a clientilor wireless prin RADIUS pe baza adresei MAC • Suport pentru RADIUS Accounting • Posibilitatea gestionarii AP-urilor remote de catre controller dar cu rutarea traficului printr-un gateway local • Wireless IDS
Functionalitati Traffic Shaping	• Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicatie si adresa IP • Suport pentru DSCP • Limitare a cotei de trafic (per adresa IP) • Suport pentru ToS
Suport instante virtuale	• Firewall/rutare per instanta virtuala • Administrare separata per instanta virtuala • Interfete VLAN separate per instanta virtuala • Politici de securitate per instanta virtuala
Suport pentru centre de date – data center	• Balansare de trafic pentru servere pe protocoalele HTTP, HTTPS, SMTPS, IMAPS, POP3S, SSL, TCP, UDP, IP • Balansare de trafic prin metode de tip: round-robin, weighted, first alive, least RTT, least session, HTTP host (din header-ul HTTP) • Persistenta sesiunilor prin metode de tip: HTTP cookie, SSL session ID • Health monitoring pentru servere fizice • Multiplexare TCP pentru sesiunile balansate • Offloading pentru SSL (preia operatiunile de criptare/decriptare de la server-ul intern pentru HTTPS si executa aceste operatii direct pe echipament) • Suport WCCP • Suport ICAP
Functionalitati High Availability - HA	• Functionare Active-Active, Active-Passive • Functionalitate Stateful Failover (Firewall si VPN) • Detectare si notificare pentru echipament nefunctional • Monitorizarea conexiunii la retea • Functionalitate Link Failover
Functionalitati de administrare, logare, autentificare a utilizatorilor	
Functionalitati de administrare	• Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI), • Posibilitatea de administrare dintr-un portal cloud-based oferit de producator • Utilizatori/Administratori cu drepturi configurabile • Functionalitate de export/import a configuratiei • Politica de control a parolelor
Functionalitati de logare si monitorizare	• Optiune de pastrare a log-urilor pe spatiu de stocare cloud-based oferit de producator • Suport syslog • Suport SNMP v1/v2c/v3 • Notificare prin e-mail pentru alerte • Suport sFlow si Netflow

Functionalitati de autentificare a utilizatorilor	• Definire locala a utilizatorilor • Integrare cu Windows Active Directory (AD) pentru Single Sign On • Integrare cu Citrix pentru autentificare SSO a utilizatorilor • Integrare cu RADIUS/LDAP/TACACS+/POP3 • Suport Xauth pentru IPSec VPN • Suport pentru autentificarea grupurilor de utilizatori prin LDAP • Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS • Suport pentru autentificare prin certificate digitale PKI X.509 • Posibilitatea limitarii accesului utilizatorilor in retea ce nu au instalat un client software de statie (client endpoint)
Conditii de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz • Consum maxim de putere: 40 W
Certificari ale sistemului de management	• ISO 9001:2015 – Managementul calitatii, pentru producator si ofertant • ISO 14001:2015 – Managementul mediului, pentru ofertant • ISO 27001:2013 – Managementul securitatii informatiei, pentru ofertant • ISO 45001:2018 – Managementul sănătăţii şi securităţii ocupaţionale, pentru ofertant; (se vor prezenta copii dupa certificatele emise de institutiile acreditate sa elibereze respectivele certificari)

Garantie si suport tehnic	• Echipamentul va include suportul tehnic de la producator:
	  ◦ Inlocuirea echipamentului in caz de defectiune hardware
	  ◦ Suport tehnic din partea producatorului de tip 24 x7
	  ◦ Update firmware versiuni minore si majore
	  ◦ Licente si update-uri de semnaturi pentru indeplinirea functionalitatilor Application Control, Antivirus/Malwave, IPS, Webfiltering si Antispam
	• Ofertantul va permite beneficiarului accesul intr-o aplicatie de tip Service Desk pe baza de user si parola.
	• Garantia si suportul tehnic se va realiza prin personalul ofertantului (minimum doi specialisti) certificat de catre producator.
	• Ofertantul va face dovada certificarii ISO 20000-1:2011 ca entitate pentru activitati de garantie, service si post-garantie.

2. Echipament integrat de protectie a retelei ce functioneaza ca o solutie de securitate unificata cu functie Wi-Fi - 8 buc.

Specificatii	**Cerinte tehnice minimale**
Specificatii hardware	• Interfete Gb-Ethernet RJ-45: 7 • Porturi consola: 1 • Porturi DMZ/WAN GbE RJ45 : 1/2 • Porturi USB: 1 • Interfata wireless: 802.11 a/b/g/n/ac
Caracteristici	• Trafic firewall (1518/512/64 byte pachete UDP): 3/3/3 Gbps • Latenta Firewall: 3 µs • Trafic Firewall masurat in pachete per secunda: 4.5 Mpps • Trafic IPSec VPN (512 byte packets): 2 Gbps

	• Trafic IPS: 400 Mbps • Trafic NGFW: 250 Mbps • Performanta SSL Inspection (IPS, HTTPS): 135 Mbps • Numar de tunele IPSec VPN site-to-site: 200 • Numar de clienti IPSec VPN: 500 • Trafic SSL-VPN: 150 Mbps • Protecția împotriva amenintarilor retelei: 200 Mbps • Numar de clienti concurenti SSL-VPN: 200 • Numar de sesiuni concurente TCP: 1.300.000 • Numar de sesiuni noi pe secunda TCP: 30.000 • Numar de politici de securitate: 5.000 • Numar de instante virtuale: 10 • Numar maxim switch-uri suportate de același producator: 16 • Numar de AP-uri total/mod tunel administrate: 30/10 • Trafic CAPWAP: 890 Mbps • Numar de token-uri OTP administrate: 500 • Numar minim de clienti endpoint administrati: 200

Functionalitati generale	• Echipament integrat de securitate cu functionalitati simultane de:
	  • Firewall de tip stateful
	  • Router cu suport pentru protocoale de rutare dinamice
	  • Posibilitate de instalare in mod bridge Ethernet
	  • Protectie Antivirus
	  • Criptare de date: IPSec VPN si SSL VPN
	  • Suport pentru QoS si Traffic Shaping
	  • Detectia si prevenirea intruziunilor – IDS/IPS
	  • Scanare si filtrare WEB – Web Inspection/Filter
	  • Blocarea si controlul traficului din retea generat de aplicatii
	  • Protectie Antispam
	  • Protectie impotriva scurgerii de informatii confidentiale
	  • Update-uri automate si in timp real
	  • Suport pentru IPv6 UTM
	  • Functionalitate de proxy SSL – posibilitatea inspectiei traficului criptat
	  • Wireless controller
	• Toate functionalitatile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum si platforma hardware apartin aceluiasi producator
	• Certificari pentru producator si produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS, Antivirus
	• Conformitate cu: CE, CB

Functionalitati securitate	
Functionalitati firewall	• Functionalitati NAT, PAT si Transparent Bridge • Optiune de a aplica NAT per politica • Suport VLAN Tagging 802.1Q • Autentificarea utilizatorilor pe grupuri • Suport VoIP SIP/H.323/SCCP Traversal NAT • Functionalitate proxy explicit HTTP/HTTPS si FTP

	• Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru functionalitatea proxy explicit • Suport WINS • Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing) • Suport pentru TCP MSS clamping • Suport pentru rescrierea campului Class of Service • Suport IPv6 (NAT/mod Transparent) • Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de statie folosit – functionalitate de tip BYOD (bring your own device) • Optiune "Scheduling" pentru politicile de firewall • Posibilitate de blocare a traficului dupa tara de origine a sursei sau destinatiei (Geo IP)
Functionalitati VPN	• Suport PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN • Criptare DES, 3DES, AES 128, AES 192, AES 256 • Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512 • Suport pentru PPTP si L2TP VPN Client Pass Through • Functionalitate "Hub and Spoke" IPSec VPN • Autentificare IKE prin certificate X.509 - suport pentru RSA si ECDSA • Suport IPSec Xauth NAT Traversal • Suport configurare IPSec automata • Functionalitate IKE Dead Peer Detection • Suport pentru RSA SecureID • Suport Single-Sign-On pentru pentru book-mark-uri portal SSL-VPN • Functionalitate Two-Factor Authentication pentru SSL-VPN • Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) • Suport tunele SSL in mod tunel si in mod portal • Suport pentru validarea clientilor SSL VPN prin verificarea aplicatiilor instalate pe statie inainte de conectare - comaptibilitate cu sistemele de operare Windows • Suport pentru autentificarea utilizatorilor de tip Single Sign On prin portalul SSL VPN • Functionalitati monitorizare tunele VPN • Producatorul are in portofoliu client de VPN IPSec si SSL propriu, care are si functionalitati de: antivirus, filtrare web, filtrare a traficului de aplicatii, scanare de vulnerabilitati
Functionalitati Antivirus	• Protectie anti-malware (virus, troian, worm, spyware, grayware) • Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, MAPI, FTP • Suport scanare antivirus Proxy-Based si Flow-Based • Suport pentru detectia malware prin sandboxing de tip Cloud-Based al fisierelor suspecte, prin achizitia unei licente suplimentare • Suport pentru carantina a fisierelor infectate • Protectie impotriva retelelor botnet si site-urilor de tip phishing pe baza de reputatie a adreselor IP si a URL-urilor accesate de utilizatori

Functionalitati filtrare trafic WEB	• Filtrare pentru protocoalele HTTP si HTTPS • Blocare a conexiunilor in functie de URL/cuvant cheie sau expresie in continutul paginilor web • Blocare a conexiunilor in functie de URL-ul din header-ul Referer al cererii HTTP • Filtrare pentru Java Applet, Cookies, scripturi Active X • Posibilitate de activare fortata a optiunii „Safe Search" pentru motoare de cautare web • Posibilitatea de modificare a header-elor HTTP din cererile generate de utilizatori • Functionalitate de monitorizare a activitatii web a utilizatorilor • Posibilitate de instiintare a utilizatorilor, prin afisarea informatiilor in cadrul unui browser web, privind paginile web blocate
Functionalitati sistem de control al aplicatiilor	• Identificarea si controlul a peste 2500 de aplicatii • Optiune de Traffic-Shaping per aplicatie • Clasificare granulara a aplicatiilor dupa criterii multiple precum: Categorii de aplicatii, Popularitate, Tehnologie si Risc • Monitorizare aplicatiilor cu rata cea mai mare de consum de banda • Monitorizarea aplicatiilor pe baza IP/Utilizator • Suport pentru decriptarea si inspectarea sesiunilor SSH • Suport pentru blocarea aplicatiilor utilizate in cadrul retelelor de tip Botnet • Posibilitate de definire a semnaturilor de aplicatie personalizate • Posibilitate de instiintare a utilizatorilor, prin afisarea informatiilor in cadrul unui browser web, privind traficul de aplicatii blocat
Functionalitati sistem de prevenire a intruziunilor/atacurilor (IPS)	• Protectie pentru peste 10000 de semnaturi de atac • Suport pentru inspectia traficului de aplicatie criptat prin protocolul SSL • Protectie pentru atacuri de tip brute force • Detectarea anomaliilor de protocol • Suport pentru semnaturi configurabile • Update-uri automate pentru semnaturi • Suport pentru IPv4 si IPv6 DDoS
Functionalitati Antispam	• Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI • Suport RBL/ORDBL • Filtrare dupa cuvinte cheie/expresie • Filtrare dupa Black/White List pentru adrese IP si e-mail
Functionalitate Data Leak Prevention	• In caz de scurgere de informatii trebuie sa permita blocarea si arhivarea conversatiei pe protocoale de email, HTTP, FTP si variantele criptate SSL; arhivarea imaginilor si a fisierelor atasate la email, transferate prin aplicatii de tip Instant Messaging , incarcate – descarcate pe un site web • Blocare dupa tip si dimensiune fisier

Functionalitati sistem de verificare a statiilor (Endpoint Control)	• Integrare cu o aplicatie software pentru securitate ce ruleaza pe statii care sa permita:
	  ◦ Blocarea traficului de aplicatii instalate pe statii
	  ◦ Restrictionarea/filtrarea accesului web
	  ◦ Scanare Antivirus

Functionalitati retea	
Functionalitati retelistica si rutare	• SDWAN-control inteligent al interfetei WAN, prin directionarea traficului prin aceasta având link-uri configurate care pot sustine peste 3000 de aplicații și utilizatori/grupuri de utilizatori. Suport pentru legaturi WAN multiple cu balansare a traficului dupa metodele: Weighted round robin a sesiunilor, impartire proportinala a volumului de trafic, prin limitarea per interfata a benzii maxime utilizabile, dupa calitatea conexiunii ISP (jitter sau latenta). • Suport PPPoE și DHCP Client/Server • Rute statice • Rutare dinamica IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS • Rutare dinamica IPv6: RIPng, OSPF v3, BGP 4+ • Gruparea interfetelor in zone de securitate • Policy-based routing • Suport VRRP si Link Failure Control • Suport VLAN Tagging (802.1q) • Suport pentru IPv6 (Firewall, DNS, SIP) • Suport One-to-One NAT • Suport NAT64, DNS64, NAT46, NAT66 • Suport LLDP
Functionalitate Wireless Controller	• Modul wireless controller pentru thin-AP-uri integrat cu urmatoarele functionalitati: • Detectie si suprimare a AP-urilor neinregistrate in controller; • Selectie automata a canalului pentru AP in functie de interferentele din mediu; • Suport pentru SSID-uri multiple; • Autentificare WEP, WPA, WPA2, WPA2 Enterprise, 802.1x • Suport Captive Portal; • Suport pentru Wireless Mesh si roaming; • Distribuire automata a clientilor wireless per AP sau banda de frecvente pentru a obtine performante optime. • Rutare dinamica a traficului generat de utilizatorii wireless prin VLAN-uri folosind autentificare prin RADIUS • Autentificare suplimentara a clientilor wireless prin RADIUS pe baza adresei MAC • Suport pentru RADIUS Accounting • Posibilitatea gestionarii AP-urilor remote de catre controller dar cu rutarea traficului printr-un gateway local • Wireless IDS
Functionalitati Traffic Shaping	• Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicatie si adresa IP • Suport pentru DSCP • Limitare a cotei de trafic (per adresa IP) • Suport pentru ToS
Suport instante virtuale	• Firewall/rutare per instanta virtuala • Administrare separata per instanta virtuala • Interfete VLAN separate per instanta virtuala

	• Politici de securitate per instanta virtuala
Suport pentru centre de date – data center	• Balansare de trafic pentru servere pe protocoalele HTTP, HTTPS, SMTPS, IMAPS, POP3S, SSL, TCP, UDP, IP • Balansare de trafic prin metode de tip: round-robin, weighted, first alive, least RTT, least session, HTTP host (din header-ul HTTP) • Persistenta sesiunilor prin metode de tip: HTTP cookie, SSL session ID • Health monitoring pentru servere fizice • Multiplexare TCP pentru sesiunile balansate • Offloading pentru SSL (preia operatiunile de criptare/decriptare de la server-ul intern pentru HTTPS si executa aceste operatii direct pe echipament) • Suport WCCP • Suport ICAP
Functionalitati High Availability - HA	• Functionare Active-Active, Active-Passive • Functionalitate Stateful Failover (Firewall si VPN) • Detectare si notificare pentru echipament nefunctional • Monitorizarea conexiunii la retea • Functionalitate Link Failover
Functionalitati de administrare, logare, autentificare a utilizatorilor	
Functionalitati de administrare	• Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI), conexiune USB • Posibilitatea de administrare dintr-un portal cloud-based oferit de producator • Utilizatori/Administratori cu drepturi configurabile • Functionalitate de export/import a configuratiei • Politica de control a parolelor
Functionalitati de logare si monitorizare	• Optiune de pastrare a log-urilor pe spatiu de stocare cloud-based oferit de producator • Suport syslog • Suport SNMP v1/v2c/v3 • Notificare prin e-mail pentru alerte • Suport sFlow si Netflow
Functionalitati de autentificare a utilizatorilor	• Definire locala a utilizatorilor • Integrare cu Windows Active Directory (AD) pentru Single Sign On • Integrare cu Citrix pentru autentificare SSO a utilizatorilor • Integrare cu RADIUS/LDAP/TACACS+/POP3 • Suport Xauth pentru IPSec VPN • Suport pentru autentificarea grupurilor de utilizatori prin LDAP • Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS • Suport pentru autentificare prin certificate digitale PKI X.509 • Posibilitatea limitarii accesului utilizatorilor in retea ce nu au instalat un client software de statie (client endpoint)
Conditii de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz • Consum maxim de putere: 16 W

Certificari ale sistemului de management	• ISO 9001:2015 – Managementul calitatii, pentru producator si ofertant • ISO 14001:2015 – Managementul mediului, pentru ofertant • ISO 27001:2013 – Managementul securitatii informatiei, pentru ofertant • ISO 45001:2018 – Managementul sănătăţii şi securităţii ocupaţionale, pentru ofertant; (se vor prezenta copii dupa certificatele emise de institutiile acreditate sa elibereze respectivele certificari)

Garantie si suport tehnic	• Echipamentul va include suportul tehnic de la producator:
	  ◦ Inlocuirea echipamentului in caz de defectiune hardware
	  ◦ Suport tehnic din partea producatorului de tip 8 x 5
	  ◦ Update firmware versiuni minore si majore
	  ◦ Licente si update-uri de semnaturi pentru indeplinirea functionalitatilor Application Control, Antivirus/Malwave, IPS, Webfiltering si Antispam
	• Ofertantul va permite beneficiarului accesul intr-o aplicatie de tip Service Desk pe baza de user si parola.
	• Garantia si suportul tehnic se va realiza prin personalul ofertantului (minimum doi specialisti) certificat de catre producator.
	• Ofertantul va face dovada certificarii ISO 20000-1:2011 ca entitate pentru activitati de garantie, service si post-garantie.