

148/1295/15.06.2017.

APROBAT,
DIRECTOR GENERAL
Stefan IONITA



15 Iun. 2017

Caiet de Sarcini pentru achizitia

„Furnizare, instalare si configurare echipamente comunicatii necesare functionarii SIEGMCR, inclusiv migrarea solutiei existente”

1. Introducere

In anul 2010 Compania Nationala de Administrare a Infrastructurii Rutiere S.A. (CNAIR) a implementat Sistemul Informatic de Emitere, Gestiune, Monitorizare si Control a Rovinietei (SIEGMCR), sistem ce permite emiterea rovinietei si a peajului urmare incasarii tarifului de utilizare a retelei de drumuri nationale din Romania (rovinietea) si a tarifului de trecere pentru utilizarea podurilor peste Dunare intre Fetesti si Cernavoda, prin intermediul unor mijloace tehnice specifice (terminale de emitere, aplicatie internet), verificarea valabilitatii achitarii tarifelor prin intermediul unor mijloace fixe sau mobile amplasate pe reseaua de drumuri nationale si colectarea/gestionarea tuturor informatiilor aferente celor doua procese mentionate, intr-un centru de date aflat in CESTRIN, sistem ce a fost extins la nivel national in anul 2012.

Descrierea beneficiarului

Autoritatea contractanta este CNAIR, denumita in continuare „Beneficiar”.

Pentru o descriere corespunzatoare a functionalitatilor componentelor solutiei si pentru a evita o interpretare eronata a cerintelor beneficiarului, in cadrul prezentului caiet de sarcini vor fi folositi si termeni consacratii din limba engleza. Solutia propusa trebuie sa aiba la baza „best practice-uri” oferite de catre producatorul/producatorii elementelor componente.

Proiectul propus are ca scop:

a) achizitionarea componentelor software si hardware necesare inlocuirii solutiei actuale, precum si a serviciilor necesare implementarii solutiei propuse.

Solutia actuala este dezvoltata pe tehnologie CISCO, echipamentul central de comunicatii fiind Catalyst 6500 si avand instalate si configurate suplimentar urmatoarele module in configuratie redundanta:

Componenta de acces ofera:

- ✦ Acces la serviciul SIEGMCR atat din medii publice cat si din medii private
- ✦ Protejarea serviciilor oferite catre public
- ✦ Acces VPN controlat pentru administratorii de sistem

Componenta de core ofera:

- ✦ Interconectarea componentelor hardware in sistem
- ✦ Conectarea serverelor de aplicatii
- ✦ Servicii de balansare pentru aplicatiile ce sunt oferite de catre beneficiar
- ✦ Protectie pentru serviciile oferite de beneficiar (web application firewall)

Solutia oferita va respecta urmatoarele **cerinte generale minime**, astfel incat aceasta trebuie sa asigure:

- ✦ infrastructura de comunicatii, hardware si software care sa sustina scopul si obiectivele prezentului proiect;
- ✦ doar echipamente noi de ultima generatie care sa beneficieze de suport din partea producatorului si sa nu fie utilizate;
- ✦ interoperabilitatea cu mediul IT administrat de beneficiar;
- ✦ licentierea software pentru toate produsele care vor rula pe infrastructura hardware;
- ✦ administrarea elementelor hardware din Acces si Core utilizand interfete de management bazate pe GUI;
- ✦ un grad inalt de securitate, asigurarea controlului accesului prin autentificarea si autorizarea administratorilor, precum si auditarea activitatii acestora;
- ✦ Documentatie necesara implementarii solutiei:
 - HLD - High Level Design
 - LLD - Low Level Design
 - NMP - Network Migrational Plan
 - NIP - Network Implementation Plan

2. Componente sistem

2.1. Subsistem - Componenta de acces securizat

Componenta de Acces trebuie sa respecte cerintele din prezentul caiet de sarcini si sa ofere o solutie tehnica adaptata la ultimele recomandari in ceea ce priveste securitatea si disponibilitatea. De asemenea, Componenta de Acces trebuie sa asigure o infrastructura hardware si software de acces securizat la serviciile publicate de catre beneficiar.

2.1.1 Echipamente de tip Next Generation Firewall (NGFW)

2.1.1.1 Rol

- ✦ Permite implementarea de zone cu niveluri de securitate diferite la nivelul Componentei de acces, controlul strict al traficului de date între acestea și asigură protecția împotriva atacurilor și încercărilor de intruziune.
- ✦ Include implementarea unei soluții de tip SSL Remote Access VPN pentru minim 25 de utilizatori de tip administrator de sistem.

2.1.1.2 Cerințe funcționale și specificații tehnice

- ✦ Implementarea de mecanisme de protecție la nivel de rețea (filtru de pachete), firewall de aplicație, mecanisme anti-intruziune (IPS) avansate ce permit generarea de recomandări cu privire la regulile de IPS ce trebuie activate/dezactivate, filtru antimalware (protecție împotriva APT, blocarea fișierelor cu reputații malicioase și posibilitatea de a trimite fișierele suspecte pentru analiză la soluții de tip sand-box atât în Cloud cât și on-premise, identificare de utilizatori și de terminale, precum și posibilitatea de decriptare a traficului de tip SSL.
- ✦ Implementarea soluției de tip SSL Remote Access VPN pentru administratori va trebui însoțită și de o soluție centralizată pentru implementarea politicilor de acces ce permite integrare cu Active Directory și permiterea accesului la SSL VPN pentru utilizatorii care îndeplinesc condițiile de securitate prestabilite (semnaturile de antivirus instalate la zi, ultimele update-uri ale sistemului de operare). În cazul în care soluția este instalată în mediul virtual, furnizorul va pune la dispoziție infrastructura hardware, aplicațiile software și licențele necesare pentru instalarea componentei ce permite implementarea politicilor de acces centralizat.
- ✦ Soluția va suporta configurații de tip failover activ-activ și activ-pasiv, și trebuie să poată fi configurată atât în modul rutat cât și în modul transparent.
- ✦ Soluția va include o aplicație de management centralizat ce permite:
 - Înregistrarea celor 2 echipamente de tip NGFW.
 - Definirea de politici de tip: access, IPS și URL filtering.
 - Centralizare evenimentelor de la senzori și permite definirea de politici de corelație pe baza acestora.
 - Descoperirea în mod pasiv a sistemelor de operare și a aplicațiilor de pe device-uri.

2.1.1.3 Configurație și dimensionare

- Configurația va fi alcătuită dintr-un modul care va include:
 - ✦ două echipamente identice din punct de vedere hardware, software și licențe;
 - ✦ fiecare echipament de tip NGFW va asigura cel puțin următoarele capacități:
 - 4 Gbps throughput de bază, în mod firewall;

- 1,2 Gbps throughput, în condiții de activare concurența a filtrelor anti-intruziune și a filtrelor per aplicație;
 - până la 1.000.000 de sesiuni sustinute, în condiții de trafic normal și în condiții de atac;
 - până la 50.000 noi sesiuni deschise, pe secundă;
 - susținerea traficului pentru 5.000 utilizatori SSL VPN concurenți;
 - posibilitatea de creare și de utilizare a 500 VLAN-uri;
 - posibilitatea de creare și de utilizare a 100 partitii interne administrativ independente;
 - interfața de management *"out-of-band"*;
 - 8 interfețe de 1Gbps, pentru trafic, cu conectorizare RJ45;
 - posibilitatea de extindere a numărului de interfețe prin adăugarea unui modul suplimentar cu 6 porturi electrice sau optice;
 - 120GB SSD intern, RAID 1;
 - surse de alimentare redundante.
- ✦ vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN;
 - ✦ configurația va include subscripțiile necesare pentru funcționalitățile de tip IPS și protecție anti-malware pe perioada asumată prin contract.

2.2. Subsistem - Componenta de core

Componenta de Core trebuie să respecte cerințele din prezentul caiet de sarcini și să ofere o soluție tehnică adaptată la ultimele recomandări în ceea ce privește securitatea și disponibilitatea. Componenta de Core trebuie să asigure o infrastructură hardware și software ce permite balansarea și protecția împotriva OWASP a aplicațiilor beneficiarului și interconectarea elementelor sistemului și a infrastructurii.

2.2.1 Echipamente de tip switch

2.2.1.1 Rol

Echipamentele de tip Switch Ethernet, cu funcții de dirijare a traficului inter-VLAN, vor fi regrupate în perechi pentru a implementa interconectarea locală a componentelor interne ale subsistemului funcțional în care se află instalate și, acolo unde este cazul, dirijarea traficului către subsistemele funcționale direct conectate.

2.2.1.2 Cerințe funcționale și specificații tehnice

Arhitectura internă și funcționalitățile echipamentelor de tip Switch Ethernet vor oferi o capacitate de comutare la viteză maximă suportată pe toate interfețele simultan, precum și comutare de tip *"cut-through"*.

2.2.1.3 Configuratie si dimensionare

Configuratia va fi alcatuita dintr-un modul care va include:

- ✦ doua pachete de echipamente identice din punct de vedere hardware, software si licente;
- ✦ vor fi incluse toate reperetele si subansamblurile necesare pentru montarea in rack, racordarea la sistemul de alimentare cu energie electrica, precum si pentru interconectarea in mediile LAN.
- ✦ Echipamentul va avea caracteristicile unui switch destinat mediului de centru de date, care sa asigure simultan urmatoarele functionalitati:
 - Switch Ethernet Layer 2;
 - Switch Ethernet Layer 3;
- ✦ Interfete fizice disponibile:
 - Minim 6 40G/100G Ethernet (cu conector QSFP) care sa suporte urmatoarele tipuri de transceivere:
 - 40GBASE-SR4
 - 40GBASE-LR4
 - 10GBASE-SR
 - 10GBASE-LR
 - 10GBASE-ER
 - 100GBASE-SR4
 - 100GBASE-LR4
 - Minim 48 1G/10G/25G Ethernet (cu conector SFP+) care sa suporte urmatoarele tipuri de transceivere:
 - 10GBASE-SR
 - 10GBASE-LR
 - 10GBASE-ER
 - 1000Base-T
 - Minim 96 100/1000/10GBase-T (care pot fi instalate si pe module interne/externe);
 - Minim 1 interfata 100Base-TX/1000Base-T pentru management „out of band”;
 - Minim 1 port consola seriala;
 - Minim 1 port USB;
- ✦ Arhitectura de tip „non-blocking”, capabila sa asigure comunicatii fara pierderi de frame-uri intre oricare doua porturi, la viteza maxima de 10/25Gbps, 40Gbps si 100Gbps, cu o intarziere minima, atat la Layer 2 cat si la Layer 3;
- ✦ Sasiu instalabil in rack de 19”;
- ✦ Kit de rack;
- ✦ Performante (per echipament):
 - Comutarea la nivel 2: minim 3 Tbps si minim 2000 Mpps;

- Tabela de adrese MAC de minim 96000 de inregistrari;
- Minim 4000 de ID-uri pentru VLAN-uri per switch;
- Procesor de control multi-core.

✦ Functionalitati minimale de nivel 2 instalate:

- Incapsulare IEEE 802.1Q;
- Rapid Per-VLAN Spanning Tree Plus sau echivalent;
- Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instante;
- Spanning Tree PortFast, Root Guard si Bridge Assurance;
- Virtual Port Channel sau o tehnologie echivalenta care sa permita crearea unui "link-aggregation group" intre doua switch-uri pe de o parte si un alt echipament de tip client (server, switch, router, etc) de partea cealalta;
- Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
- Posibilitatea balansarii legaturilor din Port Channel utilizand informatii de nivel 2, 3 si 4;
- Suport pentru "Jumbo frames" cu dimensiuni de 9216 bytes pe toate porturile;
- Mecanisme de control al inundarii retelei cu trafic unicast, multicast si broadcast;
- Private VLAN, inclusiv pe porturile de tip trunk 802.1Q;
- Suport pentru protocolul LLDP (IEEE 802.3ab);
- Suport pentru protocolul IEEE 802.3qaz (DCBX);
- Suport pentru protocolul Fibre Channel over Ethernet;
- Suport pentru protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1ad, IEEE 802.1ba, IEEE 802.3an; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames;
- VXLAN Bridge si cel putin 256 Virtual Tunnel End-Points (VTEP).

✦ Functionalitati minimale de nivel 3 instalate:

- Suport pentru urmatoarele protocoale Layer 3:
 - Open Shortest Path First (OSPF) versiunile 2 si 3;
 - Border Gateway Protocol (BGP);
 - RIP v2;
 - Multicast PIM SM, SSM si MSDP;
- Cel putin 180000 intrari in tabela de routare;
- Posibilitatea de a filtra accesul pe interfete dupa informatii despre adresa IP sursa sau destinatie si in acelasi timp si portul TCP/UDP sursa sau destinatie;
- DHCP snooping cu posibilitatea de a adauga Optiunea 82;
- Facilitatea de a filtra pe un port/VLAN a raspunsurilor la cererile protocolului ARP;
- VXLAN Routing line-rate pe toate porturile;

- cel puțin 1000 instanțe VRF.
- ✚ Funcționalități minimale de QoS:
 - Layer 2 IEEE 802.1p (CoS);
 - Configurare QoS per port;
 - Minim 4 cozi hardware de servire per port;
 - Posibilitatea de clasificare a traficului bazată pe liste de control al accesului;
 - Coada cu prioritate strictă;
 - Priority Flow Control (IEEE 802.1Qbb).
- ✚ Funcționalități de înaltă disponibilitate:
 - Surse de alimentare, ventilatoare și module de expansiune de tip "hot-swappable";
 - Surse de alimentare redundante tip "1:1";
 - Ventilatoare redundante tip "N:1".
- ✚ Funcționalități de management:
 - Suport pentru SPAN și Encapsulated Routed SPAN;
 - Suport pentru sflow sau echivalent;
 - Suport pentru revenirea la o configurație anterioară;
 - Suport pentru standardul AAA, Tacacs+ și Radius;
 - Suport pentru interfața XML (Netconf);
 - Suport pentru monitorizarea utilizării bufferelor interne;
 - Suport pentru protocolul SSHv2 și SCP.
- ✚ Parametri de alimentare (per switch):
 - 2 (două) surse AC integrate, configurabile în mod redundant ce pot fi înlocuite în timpul funcționării echipamentului, cu certificare 80 Plus Platinum;
 - Tensiunea de funcționare: 100-240 VAC;
 - Frecvența de funcționare: 50-60 Hz.
- ✚ Mediu de funcționare:
 - Temperatura de funcționare: de la 0° la 40° C;
 - Umiditate: de la 5 la 95%;
 - Fluxul de aer: dinspre spate (surse/ventilatoare) către față (porturi).

2.2.2 Echipamente de tip Application Delivery Controller - (1 pachet)

2.2.2.1 Rol

"Application Delivery Controller" (ADC), cu funcții "Load-Balancer" și "Web Application Firewall" (WAF).

[Signature]
14.06.2014

2.2.2.2 Cerinte functionale si specificatii tehnice

- ✦ O arhitectura hardware dedicata, inclusiv procesarea criptografica si compresia, care asigura integritatea procesarii, latentia specifica redusa, si care suporta tranzactionalitate ridicata in conditii de deservire cu impact liniar, inclusiv la nivel de varf de sarcina, a apelurilor autorizate de acces la resurse;
- ✦ Echipamentul va putea functiona ca proxy hardware, putand fi configurat pentru functionare stricta in mod "reverse proxy" si va integra functionalitati hardware de tip sun cookie protection.
- ✦ ADC trebuie sa poata functiona in full proxy mode si in reverse proxy mode.
- ✦ Capacitate de a procesa trafic TCP si UDP generat de diferite aplicatii.
- ✦ Multipli algoritmi sau metode de balansare a traficului: round-robin, ratio si priority (cu un numar minim de membri activi).
- ✦ Multipli algoritmi sau metode dinamice de balansare a traficului: fastest-response, least-connections, combinatia fastest-response least-connections, precum si bazate pe resursele serverelor de aplicatii (ex: utilizare CPU, incarcare memorie, gradul de incarcare al retelei etc).
- ✦ Capacitatea de a trimite cereri gradual catre serverele de aplicatii nou adaugate.
- ✦ Capacitatea de redirectare a traficului de diferite tipuri (ex: http to https)
- ✦ Monitorizarea aplicatiilor "content based", cum ar fi: HTTP/HTTPS, FTP (passiv/activ), POP3, IMAP, SIP, SMTP, telnet, RADIUS, LDAP (cu TLS sau peste canal SSL), SASP, Oracle, MSSQL, SNMP DCA, WMI, RPC si SOAP.
- ✦ Capabil sa proceseze cereri bazat pe adresa IP sursa/destinatie, SSL, hash persistence.
- ✦ Capabil sa utilizeze diferite metode pentru "cookie persistence": pasiv, insert, rewrite.
- ✦ Capabil sa utilizeze metode de persistenta a sesiunilor in functie de orice variabila din header-ul pachetelor TCP/UDP sau din payload.
- ✦ NAT (network address translation) si NAPT (network address port translation) bazat pe IP sursa si/sau IP destinatie.
- ✦ Capabilitate de a returna pachete bazata pe adresa MAC a ultimului hop (asigurarea rutarii asimetrice)
- ✦ Capacitatea de a decide directionarea traficului in functie de URL, method, HTTP host, version, cookie, tipul browser-ului folosit de client, etc.
- ✦ Capacitate de a genera reguli noi pentru managementul traficului in functie de anumite evenimente, folosind un limbaj de scripting.
- ✦ Capabil de insertie XFF in header-e HTTP, cu adresa IP originara a clientului.
- ✦ Redirectare URL catre mai multe servere virtuale in functie de HTTP response code sau URL pattern.
- ✦ Capabilitatea de a agrega si refolosi multiple sesiuni client intr-o singura sesiune server-side

- ✦ Capabilitatea de a transforma sesiuni HTTP 1.0 in sesiuni HTTP 1.1 pentru consolidarea sesiunilor server-side.
- ✦ Capabilitate de inspectie a cererilor/raspunsurilor HTTP.
- ✦ Capabilitatea de blocare a codurilor de eroare generate de anumite servere de aplicatii.
- ✦ Capabilitatea de a bloca atacuri tip DoS prin conexiuni proxy.
- ✦ Capabilitatea de a folosi ambele modele de securitate: pozitiva si negativa.
- ✦ Capabilitate de filtrare a pachetelor OSI L3-L7.
- ✦ Capabilitatea de a ascunde informatiile despre serverele de aplicatii si mesajele generate de acestea ("Resource cloaking").
- ✦ Capabilitatea de a detecta si bloca anomaliiile de protocol TCP/UDP, pentru protectie DoS.
- ✦ WAF trebuie sa aiba capacitatea de a construi in mod automat politici de securitate.
- ✦ WAF trebuie sa aiba capacitatea de a accepta prin interventie manuala fals-positives.
- ✦ WAF trebuie sa poata defini politici diferite de securitate pentru diverse aplicatii.
- ✦ Capabilitatea de definire a politicilor de blocare pentru atacuri tip DoS.
- ✦ Capabilitatea de combinare a mecanismelor detectie si de prevenire.
- ✦ Mecanism de roll-back a politicilor de securitate.
- ✦ Mecanism de versionare a politicilor de securitate.
- ✦ Mecanism de construire a politicilor de securitate real-time, cu functie de auto-invatare.
- ✦ Politici predefinite pentru diferite aplicatii (ex: MS SharePoint, Oracle Application 10g)
- ✦ Capabilitate de monitorizare a aplicatiilor protejate pentru prevenirea, detectarea si raportarea anomaliiilor de trafic precum si pentru protectia impotriva atacurilor L7 DoS.
- ✦ WAF trebuie sa suporte gruparea semnaturilor.
- ✦ WAF securitate trebuie sa suporte cel putin urmatoarele categorii de semnatuiri:
 - Baze de date: Microsoft SQL, ORACLE, MySQL, PostgreSQL, Sybase.
 - Sisteme de operare: Windows, Linux, UNIX.
 - Limbaje si contexte de aplicatie: .NET, PHP, Java.
 - Servere web: Apache, Microsoft IIS.
- ✦ Va fi posibila constructia politicii de securitate pe baza de instrumente third party de evaluare a vulnerabilitatilor - spre exemplu prin import.

2.2.2.3 Configuratie si dimensionare

Configuratia va fi alcatuita dintr-un pachet integrat hardware/software:

- ✦ fiecare pachet va include un cluster de echipamente hardware de tip "*Application Delivery Controller*" (ADC);
- ✦ fiecare cluster va include doua echipamente ADC;

[Signature]
14.06.2014

- ✦ fiecare echipament ADC va fi configurat si echipat pentru a asigura cel putin urmatoarele functionalitati:
 - 20Gbps throughput, in regim de procesare generala L4;
 - 20Gbps throughput, in regim de procesare generala L7;
 - 6Gbps compresie hardware interna integrata;
 - 10Gbps procesare criptografica hardware interna integrata;
 - 10.000 tranzactii pe secunda procesare SSL hardware interna integrata de tip RSA (cu chei 2048bit);
 - 6.500 tranzactii pe secunda procesare SSL hardware interna integrata de tip ECC (ECDSA P-256);
 - Procesarea de trafic pana la cel putin 1M cereri pe secunda L4 HTTP;
 - procesarea de trafic pana la cel putin 650.000 cereri pe secunda L7;
 - 500GB spatiu de stocare de tip HDD;
 - 8 porturi 1Gbps Ethernet SFP;
 - 4 porturi 10Gbps Ethernet SFP+;
 - doua surse de alimentare interne, in configuratie redundanta;
- ✦ fiecare echipament va fi echipat cu doua transceivere ce asigura fiecare cate un port electric de tip RJ45 si patru transceivere ce asigura fiecare cate un port optic 10Gbps (pentru fibra optica de tip MM);
- ✦ vor fi incluse toate reperele si subansamblurile necesare pentru montarea in rack, racordarea la sistemul de alimentare cu energie electrica, precum si pentru interconectarea in mediile LAN;
- ✦ configuratia va include subscriptiile de acces la actualizarile necesare WAF, reputatie si geolocalie, precum si pentru o lista dinamica de adrese IP ce pot fi surse de atacuri malitioase, pe perioada asumata prin contract.

3. Servicii

3.1 Servicii de instalare si configurare

Pentru realizarea serviciilor de instalare si configurare ale echipamentelor hardware si software se vor desfasura urmatoarele activitati:

- ✦ Instalarea si configurarea tuturor echipamentelor hardware mentionate in sectiunile anterioare;
- ✦ Instalarea si configurarea tuturor produselor software mentionate in sectiunile anterioare, inclusiv platforma hardware pe care acestea vor rula;
- ✦ Instalarea licentelor necesare punerii in functiune si activarii functionalitatilor mentionate in sectiunile anterioare;
- ✦ Livrarea patch-urilor (Cupru - cel putin cat. 5E si Fibra Optica - cel putin OM3) necesare interconectarii componentelor solutiei si conectarii cu infrastructura beneficiarului.

[Signature]
14.06.2014

3.2 Servicii de implementare

3.2.1 Cerinte generale

Scopul proiectului este asigurarea sistemului de comunicatii al SIEGMCR in vederea desfasurarii in conditii optime, de catre CNAIR, a activitatii specifice de emitere a rovinietei si a peajului urmare incasarii tarifului de utilizare a retelei de drumuri nationale din Romania (rovinieta) si a tarifului de trecere pentru utilizarea podurilor peste Dunare intre Fetesti si Cernavoda.

3.2.2 Cerinte functionale

3.2.2.1. Fluxul de acces la aplicatii

- ✦ Utilizatorul va deschide aplicatia/pagina web pentru a avea acces la aplicatia oferita de catre beneficiar;
- ✦ Conexiunile utilizatorilor la aplicatie vor traversa componentele de acces si de core, nivel la care echipamentele de tip "Next Generation FW" vor asigura in mod transparent protectia impotriva atacurilor de retea, precum si detectia si protectia anti-intruziune si antimalware;
- ✦ Functionalitatile integrate de tip "Web Application Firewall"(WAF) ale echipamentelor "Application Delivery Controller"(ADC) vor asigura in mod transparent serviciile de protectie impotriva atacurilor specifice aplicatiilor web;
- ✦ Functionalitatile integrate de optimizare a serviciilor de aplicatie, integrate la nivelul echipamentelor de tip ADC, vor asigura preluarea in hardware ("offloading") a sarcinii de procesare a compresiei si a celei de procesare criptografica SSL, precum si redistribuirea activa a sarcinii de procesare ("load-balancing") intre instantele de servere de portal sau de aplicatii;
- ✦ Functionalitatile integrate de tip "reverse proxy" ale echipamentelor de tip ADC vor asigura in mod transparent continuitatea conexiunilor intre client si serverele de aplicatii.

3.2.2.2. Disponibilitate solutie

- ✦ Fiecare echipament sa suporte configurare redundanta (failover / cluster);
- ✦ Configurarea de protocoale de rutare ce permit comutarea imediata a traficului in caz de avarie (modificarea parametrilor la nivelul protocolului de rutare care permit o tranzitie cat mai rapida);
- ✦ Conectarea duala a echipamentelor si implementarea protocoalelor necesara asigurarii unei disponibilitati ridicate;

3.2.2.3. Securitatea solutiei:

- ✦ NGFW:
 - Implementarea de liste de acces specifice fiecarui serviciu prezentat catre beneficiar;

- Implementarea de politici de tip anti-intruziune si protectie avansata impotriva continutului de tip malware;
- Implementarea de politici bazate pe reputatia dispozitivelor care acceseaza serviciile oferite de sistem;
- Implementarea de politici de corelatie care permit generarea de alerte (email, syslog) in cazul unor atacuri;
- Implementarea de politici de corelatie care permit generarea de alerte (email, syslog) in cazul unor anomalii de trafic la nivelul serverelor de aplicatii (numarul de sesiuni depaseste un prag preconfigurat);
- Implementarea solutiei de Remote Access VPN pentru administratorii de sistem, autentificarea acestora facandu-se pe baza de certificat digital si utilizatori definiti in Active Directory
- Implementarea de conditii de postura pentru administratorii care folosesc solutia de Remote Access VPN (anti-virus, update-uri de sistem de operare);
- Definirea si delimitarea zonei de test fata de zona de productie.

✦ ADC/WAF:

- Implementarea SSL offloading la nivel ADC;
- Definirea a doua zone (una de test si una de productie) care sa fie delimitate din punct de vedere logic;
- Configurarea de alerte (email) in cazul expirarii certificatelor instalate pe sistem si in cazul depasirii pragurilor de functionare normala a echipamentelor;
- Configurarea de politici de WAF (semnături) care sa tina cont de sistem de operare, baza de date si servere web utilizate pentru aplicatii;
- Configurarea de politici de WAF care sa permita accesarea stricta a anumitor tipuri de fisiere, parametri si URL-uri pe baza informatiilor oferite de catre administratorul aplicatiei.

4. Securitatea sistemului

4.1 Solutie de securizare a accesului la echipamentele de retea

Sistemul trebuie sa includa restrictionarea accesului la echipamentele de retea. Acest lucru implica definirea unor retele logice separate in functie de necesitatile de securitate ale componentelor sistemului.

Sistemul va permite auditarea accesului la echipamentele de retea, in acest sens solutia oferita va trebui sa contina o componenta care permite autentificarea utilizatorilor, autorizarea comenzilor pe echipamentele de switching, firewall si accounting. De asemenea, trebuie sa permita si autorizarea utilizatorilor la nivelul componentelor de tip ADC.

[Handwritten signature and date 14-06-2017]

In cazul unei solutii virtuale furnizorul va oferi si hardware-ul, softul si licentele necesare instalarii componentei de AAA.

Echipamentele vor fi amplasate intr-o retea logica separata de cea a utilizatorilor.

Protectia retelelor logice va fi asigurata prin intermediul echipamentelor de tip firewall. Prin intermediul acestora accesul va fi granularizat pana la nivel de IP si port.

Pentru administrarea echipamentelor solicitate in acest caiet de sarcini se vor furniza toate elementele de infrastructura necesare izolarii fizice a traficului de management de restul infrastructurii. Minim, aceasta izolare se va realiza utilizand un echipament de tip switch cu management care sa ofere minim 24 de porturi 10/100/1000 Ethernet dedicat pentru Out Of Band management si care sa poata fi integrat in solutie de autentificare, autorizare si accounting.

4.2 Sistem de identificare, autentificare si autorizare a utilizatorilor si terminalelor LAN

Pentru realizarea unui grad ridicat de securitate a infrastructurii existente, Beneficiarul doreste achizitionarea unei platforme de identificare si autorizare a utilizatorilor si terminalelor care utilizeaza servicii de Remote Access VPN. Astfel, pentru dimensionarea corecta a acestui sistem se vor avea in vedere urmatoarele cerinte:

Sistemul va fi licentiat complet pentru minim 100 de device-uri intr-o arhitectura virtualizata pentru toate functionalitatile de mai jos.

Sistemul trebuie sa satisfaca minimum urmatoarele cerinte/caracteristici/functionalitati obligatorii:

- ✦ Integrare nativa cu LDAP, RADIUS, Active Directory si RSA Authentication Manager pentru autentificarea utilizatorilor;
- ✦ Suport 802.1x, „MAC authentication bypass”, si WebAuth;
- ✦ AAA (autentificare/autorizare/accounting) pentru orice tip de terminal folosind protocolul RADIUS;
- ✦ Managementul bazei de date de utilizatori tip vizitator precum si portal captiv de autentificare customizabil;
- ✦ Managementul politicilor de criptare 802.1ae;
- ✦ Terminalele ce nu corespund politicilor de securitate vor fi asociate unui VLAN cu drepturi limitate la retea;
- ✦ Autorizarea poate contine: dVLAN, dACL;
- ✦ Solutia trebuie să ofere un client unificat pentru:
 - acces VPN folosind protocolele IKEv2 si SSL
 - politici 802.1x wired/wireless
 - IEEE 802.1AE

[Handwritten signature and date 14-06-2014]

Acest client trebuie sa fie suportat minim de sistemele de operare Windows XP, Windows 7, Mac OS X.

Strict modulul de VPN (IKEv2 si SSL) trebuie să fie suportat si de sistemele de operare mobile (iOS, Android).

Suport Radius CoA (RFC5176) pentru schimbarea dinamica a autorizarii utilizatorilor de tip WiFi sau wired.

Portal web integrat pentru autentificare centralizata de tip WebAuth atat a utilizatorilor WiFi cat si wired.

5. Training

Instruirea personalului care va asigura mentenanta solutiei va fi asigurata de catre furnizor, aceasta activitate avand un rol esential in garantarea acceptantei produselor livrate si a intregului proiect.

Beneficiarul, impreuna cu furnizorul proiectului, vor stabili de comun acord datele de inceput ale cursurilor de instruire pe baza planificarii proiectului si disponibilitatii cursantilor, durata acestora, precum si locatia de desfasurare, cu mentiunea ca locatia de desfasurare a cursurilor trebuie sa fie in Municipiului Bucuresti.

Beneficiarul va stabili lista participantilor la cursurile de instruire si va comunica responsabilului de proiect din partea furnizorului lista de cursanti.

Furnizorul trebuie sa faca dovada autorizarii instructorului de catre producatorul produselor pentru care s-a solicitat scolarizarea.

Cursurile pot incepe ulterior punerii in functiune a echipamentelor livrate, dar nu cu mai mult de 30 de zile.

Costurile aferente cursurilor vor fi in responsabilitatea furnizorul.

Instruirea se va face pe baza suportului de curs care va fi livrat fiecarui participant si care va cuprinde atat partea teoretica cat si practica pe echipamente.

La sfarsitul fiecarei sesiuni de instruire se vor elabora documentele:

- ✦ prezenta la curs;
- ✦ diploma de participare.

Cursuri administrare, referinta, operare si utilizare pentru infrastructura

Furnizorul va organiza urmatoarele cursuri:

- ✦ Curs administrare echipamente switching - 4 persoane – minim 3 zile;
- ✦ Curs administrare solutie ADC si WAF - 4 persoane – minim 5 zile;
- ✦ Curs administrare solutie NGFW - 4 persoane – minim 3 zile.


14-06-2014

6. Instalarea/migrarea solutiei

Furnizorul are obligatia de a instala, configura, integra in SIEGMCR si pune in functiune echipamentele livrate in termen de maxim **20 zile** de la data livrarii. Punerea in functiune a echipamentelor se finalizeaza cu incheierea procesului verbal de receptie.

In vederea instalarii si configurarii echipamentelor livrate, Furnizorul va avea in vedere migrarea, din punct de vedere al arhitecturii generale, a solutiei existente de comunicatii in centrul de date CESTRIN.

In vederea realizarii serviciilor de migrare, instalare si configurare, Furnizorul trebuie sa dispuna de personal tehnic specializat in tehnologiile parte integranta a solutiei actuale, cat si in solutia ce urmeaza a fi livrata si implementata. In acest sens, pentru personalul ce va participa la implementarea proiectului, vor fi prezentate documente/certificate care atesta dovedirea cunostintelor in solutiile mentionate anterior.

Beneficiarul va asigura, prin personal tehnic al administratorului serviciilor de comunicatii al CNAIR, supervizarea serviciilor de migrare, instalare si configurare, ce fac obiectul prezentei achizitii.

Beneficiarul va asigura accesul in centrul de date CESTRIN, pentru personalul tehnic al furnizorului, pana la finalizarea operatiunilor de instalare/configurare si punere in productie.

Echipamentele hardware vor fi instalate in centrul de date al beneficiarului intr-un rack de 42U ce va fi pus la dispozitie de catre furnizor impreuna cu UPS-urile necesare conform necesarului de putere al echipamentelor ce compun solutia. Rack-ul va trebui echipat cu doua PDU-uri cu conectica IEC-320 C13, IEC-320 C19 fiecare dintre ele conectate la cate un circuit electric asigurat de UPS-ul de 220V. Distributia echipamentelor in rack va fi stabilita impreuna cu beneficiarul.

Furnizorul va asigura conectica suplimentara necesara interconectarii echipamentelor (patchcord-uri/patchpanel-uri fibra optica, patchcord-uri/patchpanel-uri UTP).

Implementarea sistemului intra in atributiile furnizorului si va contine toate componentele necesare punerii in functiune a solutiei.

Furnizorul va asigura rapoarte bi-anuale de inventariere hardware si software a echipamentelor cu un tool specializat, rapoarte care vor include in mod expres notificari privind de aparitia unor imbunatatiri sau modificari aplicabile echipamentelor si software-ului aferent si privind incetarea productiei oricarui din tipurile de echipamente instalate sau privind incetarea suportului oferit de producator.

Pe baza rapoartelor bi-anuale se vor face propuneri privind imbunatatirea performantelor si dezvoltarii sistemelor de comunicatii conform ultimelor standarde internationale in materie de comunicatii de date si securitate informatica.

Furnizorul va asigura rapoarte lunare de mentenanta care sa cuprinda starea echipamentelor (module si submodule) si analiza evenimentelor la nivel de echipamente Firewall si WAF.


14-06-2014

Rapoartele / propunerile vor fi prezentate si predate catre beneficiar sub forma unor memorii tehnice in limba romana, format editabil.

Pentru situatii extraordinare furnizorul trebuie sa puna la dispozitie un sistem de colaborare audio si video „web based” cu urmatoarele capabilitati:

- “desktop sharing”;
- “web conferencing”;
- “conference session recording”.

7. Managementul proiectului si experti cheie

Furnizorul va asigura activitatea de management a proiectului, astfel incat sa se asigure respectarea graficului de activitati conform unei diagrame Gantt propusa de acesta pentru implementarea solutiei.

Pe parcursul implementarii proiectului se va preda, in format electronic, versiunea actualizata a documentelor mentionate in caietul de sarcini, precum si stadiul de realizare.

Furnizorul isi va fi indeplinit obligatiile privind activitatea de managementul proiectului atunci cand materialele livrate vor fi analizate si acceptate de catre beneficiar. Raspunsul privind acceptarea livrabilelor va fi dat in 5 zile lucratoare de la primire sau, daca este cazul, beneficiarul va furniza o lista scrisa a revizuirilor solicitate.

A. Expert comunicatii – 1 persoana

In cadrul propunerii tehnice, ofertantul are obligatia de a prezenta documente justificative ale persoanei desemnate ca expert comunicatii prin care sa probeze detinerea de competente/cunostinte in domeniul retelelor de comunicatii, de nivel expert, respectiv:

- ✦ diploma de licenta privind finalizarea studiilor superioare;
- ✦ diplome/atestare/certificari prin care se dovedeste detinerea de competente/cunostinte in domeniul retelelor de comunicatii, de nivel expert.

B. Expert securitatea sistemului – 1 persoana

In cadrul propunerii tehnice, ofertantul are obligatia de a prezenta documente justificative ale persoanei desemnate ca expert de securitate a sistemului prin care sa probeze detinerea de competente/cunostinte privind securitatea sistemelor informatice si de comunicatii, de nivel expert, respectiv:

- ✦ diploma de licenta privind finalizarea studiilor superioare;
- ✦ diplome/atestare/certificari prin care se dovedeste detinerea de competente/cunostinte privind securitatea sistemelor informatice si de comunicatii, de nivel expert.

8. Documentatie

Furnizorul va trebui sa ofere urmatoarele livrabile:

✦ HLD (High Level Design), care va cuprinde:

- Descriere sumara a solutiei ce urmeaza sa fie livrata;
- Descriere de componente ale solutiei;
- Schema logica a sistemului si descrierea acestuia.

✦ LLD (Low Level Design), care va cuprinde:

- Descrie in detaliu privind solutia ce urmeaza sa fie livrata;
- Descriere detaliata pentru toate componentele solutiei;
- Descrierea detaliata a tehnologiilor utilizate;
- Schemele logice si fizice in detaliu, modul de integrare si interconectare in detaliu (la nivel de port).

✦ NMP (Network Migrational Plan), care va include:

○ Prepararea migrarii:

- Cerinte initiale;
- Responsabilitati furnizor si beneficiar;
- Documentatie testare;
- Constrangeri;
- Rollback plan;
- Impact;
- Rezultate.

○ Migrarea serviciilor:

- Cerinte initiale;
- Operatiile ce vor fi efectuate/etapele migrarii;
- Constrangeri;
- Documentatie de testare;
- Rollback plan;
- Impact;
- Rezultate.

✦ NIP (Network Implementation Plan), care va cuprinde:

- Descriere sumara proiect si echipamente ce vor fi instalate;
- Descriere site si camera tehnica unde vor fi instalate echipamentele;
- Lista echipamente livrate;
- Instalare echipamente:
 - Masuri de securitate;
 - Tool-uri necesare instalare;

- Procedura de instalare pentru fiecare echipament.
 - Rack layout si informatii hardware pentru fiecare echipament.
 - Configuratiile echipamentelor din sistem de la momentul receptiei operationale.

Predarea documentatiei tehnice si a configuratiilor echipamentelor se face cu "Proces Verbal de predare-primire" incheiat intre Furnizor si Beneficiar.

9. Garantie si suport tehnic

Conditii tehnice si de calitate. Generalitati. Garantie.

- a. Echipamentele furnizate vor asigura cel putin parametrii solicitati in caietul de sarcini.
- b. Echipamentele furnizate vor fi noi, neutilizate si se va face dovada achizitionarii lor pe baza canalelor oficiale ale producatorilor.
- c. Conditile prezentate in acest caiet de sarcini sunt minimale si obligatorii.
- d. Echipamentele livrate vor fi insotite de declaratii de conformitate CE si certificate de garantie.
- e. Livrarea echipamentelor se va face in termen de maximum **60 zile** de la data intrarii in vigoare a contractului.
- f. Toate costurile privind transportul la sediul CESTRIN, manopera de inlocuire/remediere, manopera de configurare si integrare in SIEGMCR a produselor, sau alte costuri aditionale sunt incluse in pretul contractului.
- g. Furnizorul va trebui sa asigure garantia de buna functionare, calitatea si performantele fiecarui echipament livrat si receptionat, pentru o perioada de **3 ani** de la data receptiei calitative, consemnate in procesul verbal de receptie. Procesul verbal de receptie se semneaza la sediul CESTRIN la data punerii in functiune a echipamentelor, dupa migrarea solutiei existente, instalarea, configurarea, testarea si punerea in productie in cadrul SIEGMCR a solutiei ce face obiectul prezentei documentatii.
- h. In perioada de garantie a echipamentelor, Furnizorul are obligatia de a asigura, fara cheltuieli suplimentare din partea Beneficiarului, servicii de suport tehnic ce presupun inclusiv inlocuirea echipamentelor defecte, upgrade-uri software, remedieri de natura software. Pentru inlocuirea/remedierea defectelor aparute la echipamentele tehnice, Furnizorul are obligatia de a asigura servicii de suport 7 zile pe saptamana (Luni – Duminica), 24 ore pe zi, pe tot parcursul unui an calendaristic, inclusiv sarbatorile legale.
- i. Furnizorul are obligatia de a readuce echipamentele in starea operationala in **maximum 4 ore** de la sesizarea unei defectiuni.
- j. Reparatia este considerata finalizata in urma verificarii ca functionarea defectuoasa a produsului a fost corectata. Furnizorul are obligatia de a efectua toate operatiunile necesare punerii in functiune a echipamentului (instalare, configurare, integrare in SIEGMCR), fara costuri suplimentare din partea Beneficiarului.

- k. Toate piesele de schimb furnizate in perioada de garantie, vor fi noi si vor beneficia de aceeaasi perioada de garantie ca si echipamentele initiale si de aceleasi conditii de reparatii si suport tehnic ca si echipamentele achizitionate initial.
- l. Se solicita asigurarea urmatorului SLA (service level agreement) pe durata serviciilor solicitate:
- ✦ Furnizorul va asigura un serviciu de help-desk / management al incidentelor disponibil **24h pe zi /365 zile pe an** ca unic punct de contact pentru problemele tehnice.
 - ✦ De la momentul sesizarii unei defectiuni, serviciul de help-desk va avea un timp de raspuns initial garantat de maximum 15 minute in care furnizorul va prelua cererea de suport si va contacta beneficiarul.
 - ✦ Pentru hardware, furnizorul se obliga sa remedieze orice defectiune in maxim 4 ore de la sesizarea defectiunii.
 - ✦ Pentru defectiuni software, furnizorul se obliga sa restaureze sistemul/platforma/aplicatia la ultima configuratie stabila cunoscuta in maxim 4 ore de la sesizarea defectiunii, sa trimita catre producator, in vederea solutionarii, problemele neremediate si sa aplice patch-urile, recomandarile sau imaginile corectate primite de la acesta, conform unei programari agreeate cu beneficiarul.
 - ✦ "Service - Desk-ul" furnizorului va putea fi contactat permanent la un numar de telefon si o adresa de email pe care le va comunica ulterior procedurii de atribuire.
- m. Ofertantul declarat castigator va dovedi, in termen de 5 zile lucratoare de la data intrarii in vigoare a contractului, faptul ca acesta a incheiat contract de mentenanta si suport cu producatorul echipamentelor pentru perioada mentionata in prezentul caiet de sarcini.
- n. Se va asigura acces la o librerie electronica cu posibilitatea incarcarii de documente cu informatii de tip "Knowledge Base" (KB), care va permite crearea si stocarea de evidente privind incidentele referitoare la infrastructura de comunicatii si sistemele de securitate, cu indeplinirea urmatoarelor cerinte:
- ✦ Elementele de tip KB trebuie sa contina informatii de tipul: descrierea incidentului, data la care a aparut, data la care a fost rezolvat, persoanele care au lucrat, descrierea modalitatii de rezolvare, link-uri catre site-ul producatorului in cazul in care s-a deschis caz de suport tehnic, gravitatea incidentului, daca trebuie sau nu sa fie desemnat un incident de interes ulterior;
 - ✦ Se va asigura acces la o librerie electronica cu posibilitatea incarcarii de documente cu informatii despre echipamente sau informatii de proiectare. Libraria va fi accesata de utilizatorii beneficiarului pentru care se configureaza acest drept. Libraria va asigura functii de indexare si cautare de tip "full text" in fisiere tip Microsoft Word si Adobe PDF;

- 4 La finalul contractului, beneficiarul va putea solicita furnizorului toate documentatia stocata in acest KB, in format PDF.

10. Glosar

AAA	- Authentication Authorization Accounting
AC	- Alternating Current
ADC	- Application Delivery Controller
APT	- Advanced Persistent Threat
ARP	- Address Resolution Protocol
BGP	- Border Gateway Protocol
CNAIR	- Compania Naționala de Administrare a Infrastructurii Rutiere
CoS	- Class of Service
DCBX	- Datacenter Bridging Exchange
DHCP	- Dynamic Host Configuration Protocol
DoS	- Denial of Service
ECC	- Elliptic Curve Cryptography
ECDSA	- Elliptic Curve Digital Signature Algorithm
FTP	- File Transfer Protocol
HDD	- Hard Disk Drive
IMAP	- Internet Message Access Protocol
IPS	- Intrusion Prevention System
IT	- Tehnologia Informației
HLD	- High Level Design
HTTP	- Hypertext Transfer Protocol
LACP	- Link Aggregation Control Protocol
LAN	- Local Area Network
LDAP	- Lightweight Directory Access Protocol
LLD	- Low Level Design
LLDP	- Link Layer Discovery Protocol
MAC	- Media Access Control
MSDP	- Multicast Source Discovery Protocol
MSSQL	- Microsoft Sequence Query Language
MSTP	- Multiple Spanning Tree Protocol
NAT	- Network Address Translation
NGFW	- Next Generation Firewall
NMP	- Network Migrational Plan
NIP	- Network Implementation Plan
OSPF	- Open Shortest Path First
OWASP	- Open Web Application Security Project
PIM SM	- Protocol Independent Multicast Sparse Mode
POP3	- Post Office Protocol
QoS	- Quality of Service
QSFP	- Quad Small Form-factor Pluggable
RADIUS	- Remote Authentication Dial-In User Service
RIP	- Routing Information Protocol
RPC	- Remote Procedure Call

SASP	- Server Application State Protocol
SCP	- Secure Copy Protocol
SIP	- Session Initiation Protocol
SFP	- Small Form-factor Pluggable
SMTP	- Simple Mail Transfer Protocol
SNMP DCA	- Simple Network Monitor Data Collection Agent
SOAP	- Simple Object Access Protocol
SPAN	- Switch Port Analyzer
SSH	- Secure Shell
SSL	- Secure Sockets Layer
TCP	- Transmission Control Protocol
TLS	- Transport Layer Security
UDP	- User Datagram Protocol
URI	- Uniform Resource Identifier
URL	- Uniform Resource Locator
VLAN	- Virtual LAN
VPN	- Virtual Private Network
VRF	- Virtual Routing and Forwarding
VTEP	- Virtual Tunnel End-Points
VXLAN	- Virtual Extensible LAN
XML	- Extensible Markup Language
XFF	- X Forwarded-For
WAF	- Web Application Filter
WMI	- Windows Management Instrumentation

Intocmit:

Grup de lucru constituit prin Decizia Directorului General al CNAIR nr. 328/22.03.2017

1. Ionut MASALA - Director General Adjunct DGEF
2. Florin BUZATU - Directia Venituri
3. Catalin VLAD - Directia Venituri
4. Florin CHIOREAN - CESTRIN
5. Sorin IVANCIU - Serviciul Dezvoltare Aplicatii Interne

Viza specialitate IT

Olga Mihai
14.06.2017