ROYAUME DU MAROC
Le Chef du Gouvernement

agence nationale de réglementation des télécommunications
الوكالة الوطنية لتقنين المواصلات

CAHIER DES PRESCRIPTIONS SPECIALES

APPEL D'OFFRES OUVERT SUR OFFRES DE PRIX N°21/2021

OBJET :

ACQUISITION DE SOLUTIONS POUR LES BESOINS EN SECURITE ET RESEAU

Date limite de réception des plis : le 15/12/2021 à 11h30

PREAMBULE

Le présent appel d'offres ouvert est lancé en application des dispositions de la décision n°20/2014/DG[1] du 19 décembre 2014, telle que modifiée et complétée, fixant les conditions et les formes de passation des marchés de l'Agence Nationale de Réglementation des Télécommunications.

Entre :

L'Agence Nationale de Réglementation des Télécommunications, sise Centre d'Affaires, Boulevard Ar-Ryad, Hay Ryad, BP 2939 - RABAT 10100, représentée par son Directeur Général ou son délégataire, désignée ci-après par « ANRT ».

D'une part,

Et :

Le prestataire ou le groupement de prestataires

Désigné ci-après par « Titulaire » ou « Prestataire »,

D'autre part,

Il a été convenu et arrêté ce qui suit :

[1] Téléchargeable à partir du site Web de l'ANRT (www.anrt.ma); rubrique Appel d'Offres)

CAHIER DES PRESCRIPTIONS SPECIALES
CHAPITRE I : DISPOSITIONS GENERALES

ARTICLE 1 : OBJET DE L'APPEL D'OFFRES

Le présent appel d'offres ouvert a pour objet **l'acquisition de solutions pour les besoins en sécurité et réseau.**

ARTICLE 2 : PIECES CONSTITUTIVES DU MARCHE

Les pièces constitutives du marché comprennent :

- L'acte d'engagement,
- Le présent CPS,
- Le bordereau des prix – détail estimatif,
- La documentation technique,
- Le dossier additif ;
- Le CCAG-T.

En cas de contradiction ou de différence entre les pièces constitutives du marché, ces pièces prévalent dans l'ordre ou elles sont énumérées ci – dessus.

ARTICLE 3 : TYPE ET MONTANT DU MARCHE

Le marché découlant du présent appel d'offres est un marché unique.

Les montants ci-après du marché «ne sont pas à renseigner dans le présent document» à ce stade. Ils doivent l'être dans l'offre financière et seront transcrits dans cette partie lors de la signature du marché.

a) Attributaire national :

Devise	En dirhams marocains (MAD)
Montant de la part en MAD hors TVA	..... *(en lettres et en chiffres)*
Taux de la TVA	20 (vingt) %
Montant de la TVA	..... *(en lettres et en chiffres)*
Montant avec T.V.A comprise	..... *(en lettres et en chiffres)*

b) Attributaire étranger ou groupement constitué de soumissionnaires nationaux et étrangers :

La facturation d'une part en devise et, le cas échéant, d'une part locale est pratiquée dans le cas d'un groupement entre une (ou plusieurs) société (s) installée (s) au Maroc et une (ou plusieurs) autre (s) installée (s) à l'étranger.
La convention de groupement doit spécifier :

- le (ou les) compte (s) ouvert (s) dans une[1] banque marocaine où est versée la part locale ;
- le (ou les) compte (s) ouvert (s) dans une[2] banque étrangère où est versée la part en devise.

Un soumissionnaire étranger ou un groupement composé uniquement entre soumissionnaires étrangers doivent renseigner uniquement la part en devise.

[1] : **Pour chaque soumissionnaire national du Groupement, un seul compte est précisé.**
[2] : **Pour chaque soumissionnaire étranger du Groupement, un seul compte est précisé.**

b.1. Part en devises ($ ou €) :

Les montants facturés sont les montants hors TVA.

Pour la part en devise, une retenue à la source (RAS) prélevée sur le «montant en devise Hors TVA» ainsi que le montant de la TVA sont versés à l'administration marocaine des impôts soit :

- par l'ANRT (en cas d'accréditation), ou
- par le représentant fiscal de la société au Maroc.

En l'absence de désignation du représentant fiscal, l'ANRT se charge de verser la RAS et la TVA à l'administration Marocaine des impôts.

Une copie des reçus de versements de la RAS et de la TVA est remise à chaque soumissionnaire concerné sur sa demande.

Préciser la devise	..... *(en lettres)*
Montant de la part en devises hors TVA (*)	..... *(en lettres et en chiffres)*

(*) : Le montant qui sera payé sera celui indiqué par le Titulaire Hors TVA, duquel est déduite une Retenue à la Source (RAS), d'un montant correspondant à un taux de 10% du montant en devises Hors TVA. Cette retenue est effectuée directement par l'ANRT et versée directement à l'administration marocaine des impôts. La copie justifiant ledit versement est transmise au Titulaire à sa demande.

Exemple :

Pour un montant en devises de 100 Euros Hors TVA, le montant qui sera payé et transféré au Titulaire est de :

- 90 EUROS (= 100 - 10) : le montant de 90 EUROS correspond au montant à transférer.
- Le montant en MAD correspondant à 10 Euros est la RAS.

b.2. Part locale :

Pour la part locale, le montant à payer est le montant TTC.

Devise	En dirhams marocains (MAD)
Montant de la part en MAD hors TVA	..... *(en lettres et en chiffres)*
Taux de la TVA	20 (vingt) %
Montant de la TVA	..... *(en lettres et en chiffres)*
Montant avec T.V.A comprise (TTC)	..... *(en lettres et en chiffres)*

ARTICLE 4 : DOCUMENTS DE REFERENCE

Pour mener à bien ses missions, l'attention du prestataire est portée sur les documents suivants :

A/ Textes généraux :

- La Loi n°24-96 relative à la Poste et Télécommunications et particulièrement le titre II instituant l'Agence Nationale de Réglementation des Télécommunications promulguée par le Dahir n°1-97-162 du 2 Rabii II 1418 (7 Août 1997) et telle qu'elle a été modifiée et complétée ;
- Le Dahir n°1-15-05 du 29 rabii II (19 février 2015) portant promulgation de la Loi n°112-13 relative au nantissement des marchés publics ;
- Le Décret n°2-97-813 du 27 Chaoual 1418 (25 février 1998) portant application des dispositions de la loi n°24-96 relative à la Poste et aux Télécommunications en ce qui

23 NOV. 2021

concerne l'Agence Nationale de Réglementation des Télécommunications tel qu'il a été modifié et complété ;
- Le Décret n°2-14-394 du 13 mai 2016 approuvant le Cahier des Clauses Administratives Générales applicables aux marchés de travaux ;
- Les Textes législatifs et réglementaires en matière de législation sur les accidents du travail ;
- L'Arrêté du Ministre de l'économie et des finances n°20-14 du 8 kaada 1435 (4 septembre 2014) relatif à la dématérialisation des procédures de passation des marchés publics ;
- La Décision n°20/2014/DG du 19/12/2014 portant règlement fixant les conditions et les formes de passation des marchés de l'Agence Nationale de Réglementation des Télécommunications, telle que modifiée et complétée.

Les dispositions de ces textes et documents constituent obligation pour le Titulaire. Celui-ci ne pourra en aucun cas se prévaloir de leur ignorance pour s'en soustraire.

ARTICLE 5 : ENTITE CHARGEE DU SUIVI DE L'EXECUTION

Le suivi de l'exécution des prestations prévues par le marché issu du présent appel d'offres sera assuré par la Division chargée du Système d'Information.

ARTICLE 6 : DEVOLUTION DES ATTRIBUTIONS

Le maître d'ouvrage notifie, par ordre de service, à l'entrepreneur dans les quinze (15) jours qui suivent la date de notification de l'ordre de service prescrivant le commencement de l'exécution des travaux, le nom, la qualité et les missions de l'agent chargé du suivi de l'exécution du marché.

Toute modification ultérieure relative à la désignation de l'agent chargé du suivi de l'exécution du marché est communiquée à l'entrepreneur par ordre de service du maître d'ouvrage.

ARTICLE 7 : ELECTION DE DOMICILE

Toutes les notifications concernant le marché seront valablement faites à l'adresse précisée dans l'acte d'engagement.

ARTICLE 8 : VALIDITE DU MARCHE

Le marché ne sera valable, définitif et exécutoire qu'après son approbation par l'ANRT.

L'approbation du marché doit intervenir avant tout commencement d'exécution des prestations.

ARTICLE 9 : SOUS TRAITANCE

Les conditions de sous-traitance sont régies par les dispositions de l'article 141 de la décision n°20/2014/DG précitée.

De ce fait, la sous-traitance est une opération qui intervient dans la phase de l'exécution du marché, c'est-à-dire après que la commission d'appel d'offres ait désigné l'attributaire du marché et après que l'autorité compétente ait notifié à ce dernier l'approbation dudit marché.

Il en découle que la commission d'appel d'offres n'est habilitée à examiner que les capacités juridiques, techniques et financières du concurrent ayant présenté l'offre principale et non pas ses sous-traitants.

23 NOV. 2021

Le soumissionnaire doit justifier de ses propres capacités pour la réalisation de cette prestation et non avec celles du ou des sous-traitants.

La sous-traitance peut concerner uniquement les numéros de prix ns° 6, 7, 8, 9 et 10 sous réserve que le montant total des solutions ou équipements sous-traités ne dépasse pas 50% du montant global de son offre tel que figurant dans l'acte d'engagement du soumissionnaire.

ARTICLE 10 : DROITS D'ENREGISTREMENT

Le marché doit être enregistré par le Titulaire auprès de l'Autorité Administrative Compétente au Maroc. Dans le cas où cet enregistrement est assujetti au paiement de droits, ces derniers sont à la charge et responsabilité totale du Titulaire. L'enregistrement doit intervenir, dans tous les cas, avant le dépôt de la 1ère facture.

ARTICLE 11 : NATURE ET REVISION DES PRIX

Les prix sont fermes et non révisables.

Les prix du marché ont un caractère général conformément aux dispositions de l'article 49 du CCAG-T. Ces prix qui seront établis en dirhams comprennent le bénéfice ainsi que tous droits, impôts, frais généraux, faux frais et d'une façon générale, toutes les dépenses qui sont la conséquence nécessaire et directe des prestations de ce marché.

Ils sont réputés inclure, pour chaque numéro de prix indiqué dans le bordereau des prix-détails estimatif, tous les frais et sujétions requis pour la réalisation des prestations correspondantes. Le Titulaire ne peut se prévaloir, durant la durée du marché et pour sa réalisation, d'aucune omission ou une mauvaise estimation de la charge de travail, qui relèvent de sa totale responsabilité.

ARTICLE 12 : MODALITES DE PAIEMENT

Le règlement sera effectué après constatation du service fait pour chaque article :

- 75% à la réception provisoire.
- 15% à l'issue de la 1ère année.
- 10% à l'issue de la 2ème année.

ARTICLE 13 : REGLEMENT DES SOMMES DUES

L'ANRT se libérera des montants dus au Titulaire pour les prestations rendues et réceptionnées sous un délai de 60 jours à compter de la date du procès-verbal de réception ou de la réception de chaque facture (conforme) et de toutes les pièces justificatives exigées.
La facture doit répondre, au minimum, aux conditions suivantes :

- Être conforme au bordereau des prix - détail estimatif pour les prestations réalisées ;
- Être établie en six exemplaires originaux ;
- Être signée (par la personne habilitée) et datée ;
- Le montant de la facture doit être arrêté en chiffre et en lettres ;
- Faire ressortir les montants HT, TVA et TTC (pour les fournisseurs étrangers, elle doit faire ressortir le montant en devises Hors TVA) ;
- Indiquer l'ICE.

Toute facture ne comportant pas l'identifiant commun (ICE) de l'ANRT «ICE n°001696338000043» sera rejetée.

23 NOV. 2021

Une version électronique de la facture pourra être déposée sur la plateforme https://www.e-depot.anrt.ma.

Chaque facture doit rappeler les références du marché et l'intitulé exact du compte bancaire, l'identifiant commun du Titulaire (pour les sociétés installées au Maroc) ainsi que le RIB composé de 24 chiffres. Elle doit également reprendre l'intitulé exact des prestations exécutées. En cas d'erreur sur le RIB et en l'absence d'un avenant au marché, les paiements se feront sur le compte indiqué dans le marché signé ou, en cas de nantissement, dans le compte précisé dans l'acte de nantissement.

Le montant en devises Hors TVA sera calculé au moment du paiement sur la base du taux de change de la date de la facture.

Si le Titulaire est une société étrangère, celle-ci doit indiquer si elle a un représentant fiscal au Maroc ou accréditer l'ANRT pour effectuer les paiements d'impôts exigibles au Royaume du Maroc.

Le compte bancaire à indiquer dans la facture est comme suit :

- Si le marché fait l'objet d'un nantissement, le compte bancaire à indiquer est celui figurant dans l'acte de nantissement tel qu'il est déposé auprès de l'ANRT ;
- Si le marché ne fait pas l'objet d'un nantissement, le (ou les) compte (s) bancaire (s) à indiquer est (sont) celui (ceux) figurant dans le présent marché.

ARTICLE 14 : NANTISSEMENT

Dans l'éventualité d'une affectation en nantissement du marché, il est précisé que :

- La liquidation des sommes dues en exécution du marché sera opérée par les soins de l'ANRT.
- Le maître d'ouvrage est chargé de fournir tant au titulaire qu'aux bénéficiaires de nantissement ou subrogations les renseignements et états prévus à l'article 8 de la Loi n°112-13 relative au nantissement des marchés publics.
- Les paiements prévus au marché seront effectués par l'Agent Comptable de l'ANRT, seul qualifié pour recevoir les significations des créanciers du titulaire du marché.

L'ANRT délivrera, sans frais, au titulaire, sur sa demande et contre récépissé, une copie du marché portant la mention «exemplaire unique» et destiné à former titre pour nantissement conformément à la réglementation en vigueur, et notamment aux dispositions de la Loi n°112-13.

Dans les cas des marchés cadres ou reconductibles, si l'acte de nantissement ne permet pas d'identifier clairement si ledit acte couvre une ou plusieurs années, et à défaut de présenter une main levée de la banque bénéficiaire du nantissement, les factures présentées par le titulaire doivent être libellées en indiquant le numéro de compte bancaire figurant dans l'acte de nantissement.

ARTICLE 15 : PENALITES POUR RETARD

Lorsque les délais contractuels sont dépassés, le Titulaire encourt sans mise en demeure préalable, une pénalité par jour de retard égale à 5/1000 qui sera retenue d'office sur les sommes dues au Titulaire.
Ce taux est applicable au montant du prix concerné. Toutefois, le montant total des pénalités qui seront appliquées ne doit pas excéder 8% du montant total du marché augmenté éventuellement des montants des avenants dans le délai contractuel par jour de retard et ce, conformément aux dispositions de l'article 65 du CCAG-T.

23 NOV. 2021

Lorsque le plafond des pénalités est atteint, l'ANRT est en droit de résilier le marché après mise en demeure préalable et sans préjudice de l'application des autres mesures correctives prévues par la réglementation en vigueur.

ARTICLE 16 : CAUTIONNEMENTS PROVISOIRE ET DEFINITIF

Par dérogation aux dispositions de l'article 14 du CCAG- TRAVAUX, le titulaire est dispensé de constituer un cautionnement provisoire et un cautionnement définitif.

ARTICLE 17 : RETENUE DE GARANTIE

Par dérogation aux dispositions du CCAG-T, la retenue de garantie est fixée à 25% du montant du marché.

Chaque retenue de garantie peut être remplacée par une caution personnelle et solidaire conformément aux stipulations de l'article 17 du CCAG-T.

La retenue de garantie (soit 25% du montant du marché) est libérée, en deux phases (soit 15%, puis 10%), et ce trois mois après chacune des deux dernières échéances prévues à l'article 12 ci-dessus. La dernière est libérée après présentation des documents requis par la réglementation en vigueur pour libérer les retenus de garanties.

ARTICLE 18 : DUREE DE GARANTIE

Tous les produits et solutions proposés dans le cadre de cet appel d'offres doivent être garantis pendant une période de deux (2) années à compter de la date de chaque réception provisoire.

Pendant cette période, le Titulaire doit apporter toute son assistance technique pour le déblocage des problèmes qui pourraient survenir sur la solution objet de cet appel d'offres et ce dans un délai qui ne doit pas dépasser 24 heures. Les services suivants sont couverts par la garantie :

1. Accès au service hotline ;
2. Accès et installation des dernières versions software pour pouvoir effectuer les mises à jour mineures et majeures de la solution proposée ;
3. Renouvellement, le cas échéant, des licences ;
4. Maintenance curative (pièce et main d'œuvre) :
   - Dans un délai de 24 h maximum pour les interventions sur site et nécessitant des composantes commercialisées sur le territoire national ;
   - Dans un délai de 15 jours maximum pour les interventions nécessitant des composantes devant obligatoirement être importées de l'étranger (doit être appuyée par une justification acceptée par l'ANRT) ;
5. Maintenance Préventive :
   Trois (03) fois par an pour chaque article.

Le prestataire doit garantir un fonctionnement normal de la solution pendant toute la durée de garantie.

ARTICLE 19 : DELAI D'EXECUTION

L'ensemble des prestations objets de cet appel d'offres doit être réalisé, livré et mis en œuvre dans les locaux désignés par l'ANRT dans un délai de cent (100) jours calendaires à compter de la date de commencement mentionnée dans chaque ordre de service.

Le Titulaire fera son affaire personnelle pour le respect de ce délai compte tenu de la situation sanitaire à la date de remise de son offre.

Ce délai est entendu hors délai de validation par l'ANRT et hors délai de reprise en cas d'anomalies.

Les livraisons seront effectuées par le Titulaire à ses frais et sous sa responsabilité.

Les retards éventuels du fait de l'ANRT ne sont pas imputables au Titulaire.

Les délais de vérification, même en dépassement du délai précité, que se réserve l'ANRT pour réaliser les opérations de vérification, ne sont pas compris dans le délai d'exécution.

N.B :

- Pendant la durée des travaux, le Titulaire devra dans tous les cas assurer la continuité des services, ainsi que la sécurité des personnes.
- Les travaux nécessitant des coupures générales seront exécutés les week-ends ou en dehors des périodes de travail.

Des délais supplémentaires peuvent être pris en considération dans les cas suivants :

- Force majeure ;
- Ajournements partiels des travaux ou des livraisons ;
- Augmentation dans la masse des travaux/prestations ;
- Travaux supplémentaires, conformément aux dispositions des articles 55, 57, 58 et 59 du CCAG-T.

Les délais supplémentaires doivent se limiter strictement aux besoins nécessaires pour faire face aux cas précités.

En cas d'interruption des travaux, les dispositions des articles 48, 49, 50, 51 et 52 du CCAG-T s'appliquent.

ARTICLE 20 : LIVRABLES

Le Titulaire est tenu de produire les principaux livrables cités ci-après :

- Le planning détaillé d'exécution du projet.
- Le dossier d'ingénierie détaillant la solution à mettre en place, comprenant notamment :
  - Le diagnostic de l'existant intégrant les remarques et recommandations du Titulaire.
  - L'architecture de sécurité cible, logique et physique.
  - Le plan de migration vers la nouvelle solution intégrant le scénario de retour en arrière en cas de problème.
- Le dossier de recette détaillant les tests nécessaires à effectuer pour s'assurer du bon fonctionnement des solutions installées et de toutes leurs composantes. Ce dossier doit mentionner pour chaque cas de test les prérequis nécessaires et les résultats attendus.
- Le dossier d'administration et d'exploitation des différentes solutions mises en place, précisant notamment :
  - Toutes les règles et commandes d'installation, de configuration et de paramétrage.

23 NOV. 2021

- Une description détaillée des différentes tâches et procédures courantes d'administration (sauvegarde, restauration, analyse, logging, reporting, etc.).
- etc.

L'ANRT procède à l'appréciation des livrables produits par le Titulaire, qui doit apporter les corrections ou améliorations nécessaires dans les délais convenus avec les équipes de l'ANRT.

ARTICLE 21 : CONDITIONS DE RECEPTION

a. RECEPTION PROVISOIRE

Les prestations objets du marché sont réceptionnées après avoir vérifié leur conformité avec les spécifications exigées.

L'ANRT se réserve un délai de trente (30) jours pour prononcer la réception.

Si ces vérifications et ces essais sont jugés satisfaisants, l'ANRT prononcera la réception provisoire, en établissant un procès-verbal de réception provisoire.

Les délais de vérification, même en dépassement du délai précité, que se réserve l'ANRT pour réaliser les opérations de vérification, ne sont pas compris dans le délai d'exécution.

Le maître d'ouvrage désigne la ou les personnes pour procéder aux opérations préalables à la réception provisoire conformément aux stipulations de l'article 73 du CCAG-T.

La réception provisoire ne peut être prononcée qu'après production de l'original ou de la copie certifiée conforme à l'original des attestations du constructeur des équipements objets du marché, si ces documents n'ont pas été présentés dans le dossier additif.

b. RECEPTION DEFINITIVE

La réception définitive sera prononcée par l'ANRT, pour chaque article, à l'expiration du délai de garantie, à compter de la date de la réception provisoire, si le Titulaire a bien rempli ses engagements contractuels en matière de garantie. La dernière réception définitive vaut réception définitive du marché.

Avant de prononcer la réception définitive, si l'ANRT constate des anomalies de fonctionnement des solutions objets du marché, elle adresse au Titulaire la liste détaillée des imperfections relevées à tout moment au cours du délai de garantie. Le Titulaire est tenu d'y apporter remède dans les conditions du marché et ce, conformément aux dispositions du CCAG-T. Il retournera à l'ANRT la liste des imperfections complétées par le détail des travaux réalisés.

Si le Titulaire ne remédie pas aux imperfections dans les délais prévus conformément au CCAG-T, il est fait application des mesures prévues par la réglementation en vigueur.

Dans le cas où ces travaux ne seraient pas réalisés **deux (2) mois** après la fin de la période de garantie contractuelle, l'ANRT confisquera la retenue de garantie constituée.

ARTICLE 22 : SUIVI DES REALISATIONS PAR LE TITULAIRE ET EQUIPE PROPOSEE

Le Titulaire devra désigner le ou les interlocuteurs qui seront responsables de l'exécution du marché et du suivi des prestations avec les responsables de l'ANRT jusqu'à leur validation finale.

23 NOV. 2021

Le Titulaire devra assurer la réalisation, la livraison et la mise en œuvre des prestations objets du présent appel d'offres.

Le Titulaire aura à sa charge toutes les tâches de gestion requises pour le projet. A ce titre, il devra désigner un responsable du projet qui sera l'unique interlocuteur pour toutes les questions techniques, commerciales et administratives relatives au projet, fournir et tenir à jour un programme détaillé des travaux, participer à des réunions et produire des rapports d'avancement et compte-rendu de réunions.

Le Titulaire s'engage à donner suite à toute demande d'information permettant à l'ANRT d'assurer le contrôle du projet.

Le titulaire est, de façon générale, tenu d'informer l'ANRT de tout événement ou circonstance de nature à remettre en cause les délais assignés au projet, en vue de permettre le déclenchement d'actions correctives.

Le Titulaire participera à la réunion de démarrage qui sera organisée dès l'entrée en vigueur du marché. La réunion aura pour objet la définition des différents composants du projet, la vérification des préalables et la coordination des plannings.

L'ANRT se réserve, toutefois, le droit de demander le remplacement de tout intervenant dont les compétences et/ou le comportement seraient jugés inacceptables. Les personnes proposées en remplacement devront avoir des qualifications et une expérience jugées acceptables par l'ANRT.
Si pour des raisons indépendantes de la volonté du Titulaire, dûment justifiées, et acceptées par l'ANRT, il s'avère nécessaire de remplacer un membre de l'équipe du projet, le Titulaire proposera son remplacement par une personne de qualifications et d'expérience au moins égales et sous réserve d'acceptation par l'ANRT.

ARTICLE 23 : FRAIS DE TRANSIT ET DE TRANSPORT ET TVA A L'IMPORTATION

Au cas où le Titulaire du marché n'est pas installé au Maroc, l'Incoterm applicable à cette prestation est le DDP, Rendu Droit Acquitté, TVA non acquittée (lieu de destination convenu). Le délai qui court entre la date de livraison au niveau de l'administration des douanes et la date de paiement des droits liés à cette opération (TVA, ...) n'est pas compris dans le délai d'exécution de la prestation. Les frais afférents aux opérations de transit, transport et TVA à l'importation sont à la charge du titulaire.

L'ANRT payera uniquement la facture du titulaire après livraison et réception des prestations.

ARTICLE 24 : RESILIATION

Les conditions de résiliation du marché sont celles prévues par les dispositions de l'article 69 du CCAG-T.

ARTICLE 25 : REGLEMENT DES LITIGES

Les litiges qui se produiraient à l'occasion de l'exécution du marché sont celles prévues par les dispositions du chapitre 9 CCAG-T.

ARTICLE 26 : RESPECT DE LA CONFIDENTIALITE, SECURITE DES INFORMATIONS ET PROTECTION DES DONNEES PERSONNELLES

Le titulaire doit s'engager à respecter le principe de confidentialité et ce, par rapport aux informations qui lui seront communiquées éventuellement par l'ANRT et les autres intervenants dans le cadre de cette prestation.

Ce dernier devra aussi veiller au respect des dispositions de la loi n°09/08 relative à la protection des données personnelles dans le cadre de l'exécution des prestations objets du marché. Ce dernier ne devra en aucun cas conserver ces informations (stockage ou traitement) ou en faire usage pour son propre compte ou pour le compte d'un tiers.

Les données à caractère personnel, traitées par l'ANRT dans le cadre du marché issu du présent appel d'offres, sont utilisées pour les besoins de l'étude des offres et, le cas échéant, le suivi du marché.

Les soumissionnaires et le titulaire disposent d'un droit d'accès, de rectification et d'opposition, pour des motifs légitimes, sur les données les concernant, conformément à la réglementation en vigueur. Pour exercer ce droit, ils doivent s'adresser :

- par voie postale à : Secrétaire Général de l'ANRT, Centre d'affaires, Boulevard Ar-Ryad, Hay Riad – BP:2939, Rabat.
- ou par courrier électronique à : ao-DP-anrt@anrt.ma.

Le présent traitement est autorisé par la CNDP sous l'autorisation n°A-GF-161/2013 du 1er novembre 2013.

ARTICLE 27 : LUTTE CONTRE LA FRAUDE ET LA CORRUPTION

Il sera fait application des articles 25 et 151 du règlement des marchés de l'ANRT.

Le Titulaire ne doit pas recourir par lui-même ou par personne interposée à des pratiques de fraude ou de corruption des personnes qui interviennent, à quelque titre que ce soit, dans les différentes procédures de passation, de gestion et d'exécution du marché.
Le Titulaire ne doit pas faire, par lui-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion du marché et lors des étapes de son exécution.
Les dispositions du présent article s'appliquent à l'ensemble des intervenants dans l'exécution du présent marché.

CHAPITRE II : DISPOSITIONS PARTICULIERES

ARTICLE 28 : CONSISTANCE DES PRESTATIONS

PREAMBULE

Le présent appel d'offres ouvert a pour objet la mise à niveau des solutions de sécurité et de réseau du Système d'Information de l'Agence Nationale de Réglementation des Télécommunications. La plateforme de sécurité proposée devra comprendre la fourniture et la mise en place des composantes suivantes :

- Plateformes de Pare-feu nouvelle génération en haute disponibilité, pour les parties frontale et dorsale. La plateforme de Pare-feu frontale et celle de Pare-Feu dorsale doivent être de marque et technologies différentes ;
- Plateforme WAF (Web Application Firewall), en haute disponibilité, pour la protection des applications web contre l'exploitation des vulnérabilités connues et émergentes ;

23 NOV. 2021

- Plateforme de passerelle de messagerie, avec licences antispam et antivirus, en haute disponibilité ;
- Plateforme de contrôle d'accès au réseau, en haute disponibilité ;
- Switch d'étage à 48 ports ;
- Switch à 24 ports ;
- Equipement pour gestion de flux Internet ;
- Solution de sécurité email pour Microsoft Exchange.

ARTICLE 1 : CONSISTANCE DES PRESTATIONS

Dans le cadre de l'amélioration et la mise à niveau continue des plateformes de sécurité et de réseau de son Système d'Information, l'ANRT lance le présent appel d'offres ouvert pour l'acquisition, l'installation et la mise en service de solutions de sécurité et de réseau.

Le présent cahier des charges décrit les caractéristiques techniques des solutions demandées ainsi que le détail des prestations à réaliser.

Tout équipement livré doit être compatible au protocole IPv6 et au protocole IPv4.

Toutes les prestations ci-après incluent, pour chaque article, fourniture, installation, paramétrage, configuration, support, garantie et formation ou transfert de compétences.

1. Caractéristiques minimales des solutions à déployer :

Les solutions fournies doivent respecter les spécifications minimales ci-après, en présentant un tableau de conformité avec spécification et réponse du soumissionnaire (cf. annexe).

1.1. Article N°1 : Pare-feu frontal Nouvelle Génération

Le soumissionnaire doit proposer une solution redondante de firewall frontal de nouvelle génération NGFW, conçue pour protéger l'infrastructure réseau, améliorer la connectivité entre sites et simplifier l'administration des opérations sur le réseau.

La solution doit intégrer un ensemble complet de technologies de dernière génération en matière de pare-feu, contrôle d'applications de niveau 7 et prévention des intrusions.

La solution proposée doit être dotée de fonctionnalités intelligentes de gestion du trafic entre sites qui optimisent à la fois la disponibilité et les performances du réseau étendu (WAN). La solution proposée doit offrir la possibilité de contrôler le routage au niveau des applications ainsi que les priorités données au trafic sur plusieurs liaisons, tunnels et conditions de trafic.

Dans le cas où la solution n'intègre pas son outil d'administration, le Titulaire est tenu de fournir, à sa charge, la solution d'administration ainsi que les prérequis nécessaires à son installation et qui deviennent propriété de l'ANRT.

Au cas où la solution d'administration proposée serait sous forme logicielle, elle devra être compatible avec la solution de virtualisation de l'ANRT.

Les fonctionnalités minimales à proposer sont comme suit :

Désignation	Spécifications minimales
Type de Firewall	Firewall de nouvelle génération offrant les services Statefull Firewall.
Positionnement	Recommandé sur le dernier rapport NSS-Labs NGFW avec un score supérieur à 95% ou Leader sur l'un des trois derniers rapports Gartner Enterprise Network Firewall.
Quantité	Deux (2) boitiers.

23 NOV. 2021

Format Boitier	Appliance Rackable 19 pouce 1 RU
Performances	Débit NGFW : Minimum 3 Gbps
	Nombre de connexions simultanées avec inspection : 1 million
	Débit d'inspection TLS : Minimum 450 Mbps
	Débit IPsec VPN 1 Gbps
Interfaces	Chaque boitier doit supporter au minimum 8 ports 1GE RJ45.
Fonctionnalités	Module Firewalling statefull pour assurer le filtrage et inspection des flux entrants et sortants en IPv4 et IPv6
	Filtrage par id utilisateur et par application
	La solution doit permettre la création de règles de sécurité granulaires à base d'adresse IP/Réseau, nom/groupe d'utilisateur, Service, protocoles, Applications, Domaine, FQDN, Pays/continent et profil d'inspection approfondie…
	Permet la prise en compte de la géolocalisation des connexions sortantes et entrantes dans les règles.
	Déchiffrement et analyse des SSL/TLS entrants et sortants
	Possibilité d'exclure un flux du déchiffrement
	Doté du module d'antimalware afin de traquer en temps réel les virus, vers, chevaux de Troie, Botnet, autres menaces avancées.
	Inspection des protocoles http, https, ssh en mode proxy pour contrôler les paramètres des protocoles L7
	Protection contre les attaques de déni de service
	Support de la détection des scans réseaux
	Protection efficace contre les intrusions par IPS
	Analyse des flux et contenu sur la base des signatures et réputation
	Translation d'adresses NAT, PAT et NAT à base de règles
	Routage statique et dynamique (OSPF, RIP, BGP)
	Gestion de la QoS : priorisation des flux, limitation et réservation de bande passante
	Haute disponibilité en mode Actif/Actif ou Actif/Passif
	Offre VLAN tagging
Licence	Licence (IPS, Antimalware, Control APP) pour 2 ans
Administration et reporting	Authentification : Radius, Tacacs+ et Active Directory pour les utilisateurs avec possibilité de couplage avec les solutions d'authentification forte
	La solution doit offrir un management centralisé via une interface d'administration et de reporting unique
	Gestion des sauvegardes et restauration de la configuration
	Centralisation du téléchargement et déploiement des mises à jour des signatures, des correctifs et des patchs
	Support SNMPv3
Licence/garantie/support	2 ans

23 NOV. 2021

1.2. Article N°2 : Pare-feu dorsal Nouvelle Génération

Le soumissionnaire doit proposer deux (2) firewalls dorsaux de nouvelle génération NGFW, en mode HA. **Le Firewall dorsal doit être de marque et technologie différente que le Firewall Frontal.**

Dans le cas où la solution n'intègre pas son outil d'administration, le Titulaire doit fournir, à sa charge, la solution d'administration ainsi que les prérequis nécessaires à son installation et qui deviennent propriété de l'ANRT.

Au cas où la solution d'administration proposée serait sous forme logicielle, elle devra être compatible avec la solution de virtualisation de l'ANRT.

Les spécifications minimales à proposer sont citées ci-après :

Désignation	Spécifications minimales
Positionnement	Firewall Nouvelle Génération, Leader sur l'un des trois derniers rapports Gartner Enterprise Network Firewall ou recommandé dans le dernier rapport NSS Labs NGFW avec une protection supérieure à 95%.
Type de Firewall	Firewall de nouvelle génération offrant les services Statefull Firewall
Quantité	Deux (2) boitiers au niveau du site principal
Format Boitier	Appliance Rackable 19 pouce 1 RU
Performances	Débit NGFW 5 Gbps.
	Un débit Inspection TLS 3 Gbps
	Un débit VPN IPsec 10 Gbps
	Support de 200 000 nouvelles connexions TCP par seconde ;
	Support de 4 millions de connexions TCP simultanées ;
	Permet le stockage en local ou dans l'outil d'administration avec une capacité minimale de 2 disques de 240 Gb SSD
Interfaces	Doté au minimum de 12 ports réseaux 1GbE RJ45; Doté au minimum de 2 ports réseaux 10GbE SFP+
Haute Disponibilité	Support la haute disponibilité en mode Actif/Passif et en mode Actif/Actif Clustering ;
	Partage de charge entre les firewalls du cluster
Fonctionnalités	Module IPS (prévention des intrusions) pour se protéger contre les menaces réseau (vers, chevaux de Troie ..). Le module IPS doit aussi apporter une protection contre les menaces réseaux existantes et émergentes, à travers deux mécanismes de détection (par signatures et par anomalies).
	Module Filtrage de contenu pour assurer le contrôle de l'accès interne aux contenus Web indésirables ou illégaux ;
	Filtrage en fonction de l'adresse source, adresse destination, utilisateur, service, protocole, interface d'entrée, Type de Device...
	Identification des applications dans le réseau, détection et protection contre les communications réseau malveillantes et dangereuses.

23 NOV. 2021

	Supporte la création des règles de firewall basées sur l'identité de l'utilisateur en plus d'autres critères : Source/Destination, IP/Sous Réseau, Port Source/Dest ....
	Gestion des plages d'adresses, des groupes d'IPs (machines, réseaux, plages d'adresses), des groupes d'utilisateurs, groupes de services...
	Possibilité de visualiser et de désactiver les règles implicites.
	Possibilité d'appliquer et d'associer des règles QoS aux règles de firewall (ACL) ;
	Possibilité de gestion de la bande passante par application.
	Support du Policy Based Routing
	Supporte de l'IPV6 ;
	Support le VPN IPsec Site to Site, Client to Site et le SSL VPN client to site
	Routage statique et dynamique (OSPF, RIP, BGP)
Licence	Licence pour 2 ans incluant les services (Contrôle applicatif, IPS, antivirus, antimalware VPN IPSec et SSL) ;
Administration et reporting	La solution doit offrir un management centralisé via une interface d'administration et de reporting unique. Gestion centralisée des sauvegardes et restauration des configurations
Licence/garantie/support	2 ans

1.3. Article N°3 : Web Application Firewall

Le soumissionnaire doit proposer une solution redondante de protection des applications web contre l'exploitation des vulnérabilités connues et inconnues.

La solution proposée par le prestataire devra répondre aux fonctionnalités minimales suivantes :

Désignation	Spécifications minimales
Positionnement	Challenger ou leader sur l'un des deux derniers rapports Gartner WAF;
Quantité	Deux (2) boitiers.
Performances	Support d'un throughput HTTP/HTTPS d'au moins 2 Gb/s
	Doté d'au moins 4 ports 1 GbE RJ45 avec la fourniture de leur SFP
	Doté d'un espace de stockage d'au moins 400 GB;
	RAM : 16 GB
	Accélération Hardware SSL : 2 000 Transactions par seconde
Fonctionnalités	Doit être capable de gérer le trafic IPv4 et IPv6
	Support de la Haute disponibilité Actif/passif et Actif/Actif Clustering.
	Support de la répartition de charge Niveau 7
	Offre l'accélération Hardware du flux SSL/TLS
	Protection contre les attaques des applications web comme : OWASP Top 10

23 NOV. 2021

	Protection contre le DoS et DDoS applicatif
	Inclure des mécanismes de cryptage des données au niveau de la couche 7 pour protéger les clients contre les logiciels malveillants et les Key Loggers.
	Proposer des mécanismes d'atténuation (Limitation du nombre de requêtes, Blocage de requêtes...).
	Utilisation du moteur d'apprentissage automatique.
	Fournir des templates ou assistant de configuration pour les applications standards.
	Protection FTP et SMTP.
	Nombre d'applications illimité.
	La solution doit être capable de détecter et de contenir les attaques ayant notamment pour objectif de découvrir les vulnérabilités d'un site Web.
	Protection contre le mécanisme d'évasion.
	Protection Antivirale notamment via ICAP.
	Offre la validation de la conformité JSON et XML
	La solution doit disposer de mécanismes d'apprentissage automatique de la structure et des éléments d'une application Web.
	Offre la protection par IP Réputation et IP Géolocalisation
	Supporter la Protection contre les attaques automatisées et détection de botNET
Licence/garantie/support	2 ans

1.4. Article N° 04 : Passerelle mail sécurisée

Le soumissionnaire doit fournir la solution matérielle redondante et les licences nécessaires pour sécuriser la messagerie au niveau de la passerelle.

La solution proposée doit répondre aux fonctionnalités minimales suivantes :

Désignation	Spécifications minimales
Positionnement	Leader dans le dernier rapport « Gartner Magic Quadrant for Secure Email Gateway »
Quantité	Deux Boîtiers physiques en haute disponibilité.
Caractéristiques matérielles minimales	• Processeurs : 1 x 2.1 GHz, 8 core, 2400 Mhz • Mémoire : 16 GB DDR4 • Disque : 1 TB • Interface réseau : 2 ports 1 GE RJ45 • Format appliance 19" ou 1RU
Dimensionnement	Licence pour 500 boîtes de messagerie. La licence doit comporter la protection antivirale, antispam, protection contre les attaques avancées et filtrage par réputation.

23 NOV. 2021

Spécifications Fonctionnelles	• Relai SMTP intégré ; • Protection Anti-spam ; • Protection contre les malwares avancés (AMP) • Système de réputation dynamique ; • Protection anti-virale (basé sur signature / zero-hour) ; • Protection anti-phishing ; • Protection contre les attaques ciblées (URL et Pièce-jointe) ; • Protection contre les faux e-mails de notification d'erreur; • Filtrage du contenu des e-mails entrants et sortants : Bloquer (ou modifier) les messages qui contiennent des mots ou expressions spécifiques enfreignant une règle de contenu définie ; • Scan en temps réel du protocole SMTP. • Data loss protection (DLP) pour se protéger contre la fuite des données confidentielles par le canal mail ; • Cryptage des emails. • Supporter les protocoles de messagerie SMTP, ESMTP, Secure SMTP sur TLS ; • Règles personnalisables pour scanner les messages et les pièces jointes entrants et sortants ; • Détection de macros dans les pièces jointes. • Stratégies flexibles pour cibler les expéditeurs ou les destinataires par entreprise, par groupe ou par individu ; • Gestion des autorisations, filtrage, mise en quarantaine, blocage, notification et reporting ; • Intégration avec LDAP pour la validation des adresses des destinataires ; • La solution doit supporter la prise en charge de la remédiation automatique sur les serveurs Exchange 2016/2019 pour les fonctionnalités et actions rétrospectives.
Filtrage de contenu	La solution doit, aussi, permettre : • La protection contre les attaques et email frauduleux ; • Une analyse multicritère des messages afin de détecter les courriers indésirables ; • Le filtrage en temps réel du contenu des e-mails ; • Application des règles de filtrage en se basant sur les caractéristiques des pièces jointes, des lexiques, et d'autres identifiants (adresse mail interne/externe...).
Filtrage antispam/antivirus	• Le moteur anti-spam doit pouvoir utiliser un moteur pouvant s'appuyer sur plusieurs caractéristiques du message afin de qualifier le message de spam ; • La protection contre les menaces mixtes, virus, chevaux de Troie, vers, programmes espions, Url malveillant, logiciels publicitaires, spam, phishing; • La protection multicouche avec un service de gestion dynamique de la réputation des emails pour bloquer les connexions à partir des adresses IP malveillantes ; • Une détection efficace des menaces, du spam et des attaques ciblées (spear phish, codes malicieux) ; • Une protection contre les virus et les infections à travers : o Une protection antivirus « zero-hour ». o Identifier la disposition d'un fichier (propre, inconnu ou

23 NOV. 2021

	malicieux). o La solution doit être capable de pré-classifier les fichiers afin de juger de leur pertinence à être transmis pour analyse dynamique ou pas. o La solution doit être capable de traker le changement de disposition d'un fichier (un fichier propre ou inconnu qui devient malicieux). o Possibilité de vérifier les URLs dans les pièces jointes • Capacité de pouvoir aussi s'intégrer à un sandboxing. • Une liste noire dynamique bloquant les messages entrants en fonction de l'adresse IP, du domaine ou de l'adresse e-mail ; • Une liste blanche définie par l'administrateur (expéditeur, relais, nom de domaine). • Le blocage et la mise en quarantaine des messages accompagnés de pièces jointes ou d'URL malveillantes afin qu'elles n'atteignent pas la boîte de réception.
Administration et reporting	• Administration aisée par interface graphique en HTTPS ou en ligne de commande via SSH. • Possibilité d'administration à distance. • Configuration flexible des politiques de sécurité. • Mise en place de quarantaines différentes pour (les messages détectés comme spams, les messages infectés pas des virus, les messages mis en quarantaine par un filtre de contenu). • Support des services : LDAP, DNS, NTP, http/https, SSH, FTP, SCP, SNMP • Génération automatique des rapports (tableaux de bord) qui sont envoyés automatiquement aux administrateurs.
Licence/garantie/support	2 ans

1.5. Article N° 05 : Contrôle d'accès au réseau

La solution à proposer devra assurer les contrôles d'accès des utilisateurs et des postes de travail au réseau ainsi que la conformité par rapport à la politique de sécurité.

La solution proposée par le prestataire devra répondre aux fonctionnalités minimales suivantes :

Désignation	Spécifications minimales
Positionnement	Leader dans le dernier rapport Gartner de solutions de contrôle d'accès réseau.
Caractéristiques	• Format rackable • CPU 8-core, 2.10 GHz minimum • 32 GB de RAM minimum • 1 Disque Dur SAS de 600 GB minimum • Interfaces réseaux nécessaires au déploiement : 4 x 1GBase-T
Appliance	Deux Boîtiers physiques en haute disponibilité
Dimensionnement	500 clients simultanés.
Authentification	• L'authentification de l'utilisateur doit se faire par :

23 NOV. 2021

	○ Authentification 802.1X standard ○ Authentification Web en mode Centralisé ○ MAB : Mac Address Bypass • La solution doit pouvoir fonctionner comme serveur RADIUS. Elle devra permettre la construction des règles d'authentification et autorisation (politiques) et permettre de configurer des groupes de politiques. • La solution doit distinguer si la requête provient d'un équipement d'accès wifi (RADIUS NAS-Port-Type = Wireless – IEEE 802.11) et si l'authentification est de type 802.1X (RADIUS Service-Type = Framed), MAB (RADIUS Service-Type = Call Check) ou même pour ouvrir une session d'administration Telnet/SSH sur un équipement réseau (RADIUS Service-Type = Login). • La solution devra supporter la liste des protocoles d'authentification suivants : ○ Host lookup / MAB ○ PAP / ASCII ○ CHAP ○ MS-CHAPv1, MS-CHAPv2 o EAP-MD5 ○ EAP-TLS ○ EAP-TTLS (depuis la version 2.0) ○ LEAP ○ PEAP (MS-CHAPv2, EAP-TLS et EAP-GTC) ○ EAP-FAST (MS-CHAPv2, EAP-TLS et EAP-GTC) • La solution doit permettre la possibilité de faire une authentification double « machine + utilisateur » au sein d'une même authentification (EAP-Chaining)
Annuaires pour le contrôle d'identité	La solution devra pouvoir s'appuyer sur sa base interne (équipements ou utilisateurs) ou bien une base externe. La solution devra supporter différents types de base externe : • Ms Active Directory (2016, 2019) • Serveurs LDAPv3 • Serveur Radius Externe • Serveur de certificats d'entreprise • SAML pour les portails Web (Oracle Access Manager par exemple)
Autorisation	Les règles d'autorisation doivent pouvoir être construites en évaluant des conditions. La solution doit avoir le concept de « Policy Sets » permettant de configurer des groupes de politiques d'authentification et d'autorisation, en séparant notamment les règles pour l'accès wifi de celles pour l'accès filaire ou VPN. La solution doit pouvoir intégrer des profils d'équipements réseaux adaptés à différents constructeurs.
Accès invité	L'accès invité doit être inclus dans la solution. La solution doit disposer de base d'une fonctionnalité Guest complète avec différents portails WEB : • Portail Guest • Portail Sponsor (création des comptes) • Portail BYOD (enregistrement des équipements) • Portal Self registration (pour les invités qui veulent créer leur propre compte) • Portail MDM (pour l'interaction avec les MDM)

	Le renvoi vers un de ces portails est effectué via une URL de redirection qui est envoyée via la solution à un commutateur ou un contrôleur Wireless. L'utilisateur sera automatiquement redirigé vers la page du portail lorsqu'il ouvrira une page web. L'ensemble des pages du portail web doivent être entièrement personnalisables via l'interface de la solution.
Authentification des invités	La solution doit supporter les annuaires ci-après, pour la vérification des coordonnées d'un invité à travers le portail captif : Interne : l'annuaire standard où l'administrateur peut créer des utilisateurs à tout moment. Externes : les annuaires MS AD, Radius et LDAP. Guest : un annuaire interne, les utilisateurs étant créés directement par les sponsors ou par les invités eux-mêmes à travers la procédure de self-service qui permet aux invités d'auto-enregistrer leurs noms d'utilisateur et mots de passe. Les utilisateurs doivent pouvoir être authentifiés soit vers les annuaires interne et externe, soit vers l'annuaire Guest, soit vers les trois en spécifiant une séquence d'annuaires à interroger.
Création des comptes dans la base de données locale 'Guest'	L'utilisation de la base de données locale Guest doit permettre de collecter un certain nombre d'informations sur les invités et de leur assigner un groupe ainsi que des limites horaires de connexion.
Profiling	La solution doit supporter la fonction de profiling permettant de classifier les équipements selon les données contenues dans plusieurs types de trafic en fonction de leur provenance.
Contrôle de conformité	A travers différents types d'agents installés au niveau du poste de travail, la solution doit supporter la vérification de plusieurs règles de conformité pour contrôler si un antivirus a été installé, si sa version est mise à jour, si certains services ou applications fonctionnent correctement sur le poste de travail, etc. Selon l'état de conformité du poste de travail, il est possible de lui garantir un niveau d'accès spécifique, ou éventuellement lui assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation. Le contrôle de conformité du poste de travail doit porter au minimum sur : • Niveau des patchs des systèmes Microsoft Windows 7, Windows 8, Windows 10. • Contrôle des MAJ des listes des définitions des virus pour les principaux Antivirus. • Contrôles des services non essentiels pour les postes de travail et qui présentent un danger : Service Serveur Web, Serveur FTP et Serveur Telnet. L'administrateur doit pouvoir décider si la remédiation est obligatoire ou optionnelle, manuelle ou automatique.
Monitoring & Reporting	• La solution devra fournir un tableau de bord (dashboard) affichant des métriques temps réel des utilisateurs et terminaux connectés au réseau. • La solution doit permettre de générer des rapports en utilisant des modèles prédéfinis et personnalisables. • La solution doit permettre de générer plusieurs types de rapports, notamment sur les performances du système, opérations d'administration,

23 NOV. 2021

	• Authentification Radius… • Les rapports doivent être exportables en format CSV ou PDF.
Licence/garantie/support	• 2 ans

1.6. Article N°06 : Switch d'étage à 48 ports

Les Switch proposés doivent répondre au minimum aux caractéristiques suivantes :

Désignation	Spécifications minimales
Format	Châssis Rackable 19"
Ports	• 48 ports 10/100/1000 Mbps PoE+ • 4 ports 1 Gigabit Ethernet SFP
Performances	• 2 GB de DRAM • 4 Go de Flash • Capacité de commutation d'au moins 100 Gbps (IPv4) • Jusqu'à 3 000 entrées de routage IPv4
Protocoles	Support des protocoles Niveau 2, RIPv1, RIPv2, RIPng, OSPF (Accès routé), PBR, PIM Stub Multicast, PVLAN, VRRP
Fonctions de sécurité	Support du protocole standard 802.1ae MACSec-128 permettant la sécurisation de la couche MAC.
SNMP	v1, v2c, and v3
Fonctions d'automatisation	NETCONF/YANG, RESTCONF, PnP
Alimentation	Un bloc d'alimentation avec possibilité d'ajouter un deuxième bloc.
Licence/garantie/support	2 ans

1.7. Article N°07 : Switch à 24 ports

Les switchs proposés doivent répondre au minimum les caractéristiques suivantes :

Désignation	Spécifications minimales
Format	• Châssis Rackable 19"
Ports	• 24 ports 10/100/1000 Mbps • 4 ports 1 Gigabit Ethernet SFP
Performances	• 2 GB de DRAM • 4 Go de Flash • Capacité de commutation d'au moins 50 Gbps (IPv4) • Jusqu'à 3 000 entrées de routage IPv4
Protocoles	Support des protocoles Niveau 2, RIPv1, RIPv2, RIPng, OSPF (Accès routé), PBR, PIM Stub Multicast, PVLAN, VRRP
Fonctions de sécurité	Support du protocole standard 802.1ae MACSec-128 permettant la sécurisation de la couche MAC.
SNMP	v1, v2c, and v3
Fonctions d'automatisation	NETCONF/YANG, RESTCONF, PnP
Alimentation	Un bloc d'alimentation avec possibilité d'ajouter un deuxième bloc
Licence/garantie/support	2 ans

1.8. Article N° 08 : Equipement pour la gestion de flux Internet

L'ANRT dispose d'un équipement qui assure le service de répartition de charge entre les liens Internet. Afin d'assurer une haute disponibilité de ce service, le Prestataire devra proposer un second équipement pour fonctionner en HA avec l'équipement actuel[2] (F5 BIG-IP i2600) dont dispose l'ANRT. L'équipement proposé doit être compatible avec l'équipement actuel précité.

Cet équipement devra répondre aux caractéristiques minimales suivantes :

Désignation	Spécifications minimales
Format	Appliance rackable 19 Pouces
Performances	• Local Traffic Manager (LTM) • Mémoire: 16 GB • Processeur: 1x deux core Intel Xeon • Débit 10 Gbps L4/L7
Module DNS	Module DNS (GSLB, DNS, DNSSEC)
Ports	4 SFP 1000BASE-T Transceiver
Alimentation	Un bloc d'alimentation avec possibilité d'ajouter un deuxième bloc
Licence/garantie/support	2 ans

1.9. Article N° 09 : Solution de sécurité email pour Microsoft Exchange

La solution à proposer devra assurer la sécurité de la solution de messagerie Microsoft Exchange déployée par l'ANRT. La solution proposée par le prestataire devra répondre aux fonctionnalités minimales suivantes :

Désignation	Spécifications minimales
Positionnement	Leader dans le rapport The Forrester Wave™: Enterprise Email Security, 2021.
Dimensionnement	500 comptes.
Fonctionnalités	• La solution doit : ✓ Utiliser les techniques de détection les plus avancées, y compris l'apprentissage automatique prédictif et la détection des exploitations de documents, pour détecter les menaces inconnues dans les fichiers, les macros et les scripts ; ✓ Détecter et prendre des mesures contre les virus / programmes malveillants, chevaux de Troie et vers ; ✓ Être capable de rechercher et de détruire les e-mails en fonction du sujet, de l'expéditeur ou du destinataire du courrier ; ✓ Bloquer les e-mails avec des URL malveillantes avant la livraison et ré-analyse les URL en temps réel lorsqu'un utilisateur clique dessus ; ✓ Prendre en charge la stratégie (DLP) pour éviter la perte de données et les violations de conformité avec des stratégies pré-prédéfinies, utilisant des mots-clés, des expressions régulières et des identifiants régionaux ; ✓ Fournir des stratégies de pièce jointe pour bloquer les pièces jointes nommées ou bloquer les pièces jointes par vrai type de fichier,

[2] : Le soumissionnaire peut proposer, à sa charge, le remplacement de celui existant chez l'ANRT ainsi que les prestations de re-paramétrage et de mise en fonctionnement.

23 NOV. 2021

	extension de fichier ou nom de fichier, avec des règles d'exception intégrées à Active Directory ; ✓ Fournir une règle de filtrage de contenu basée sur des mots clés et des expressions régulières pour filtrer le contenu des messages jugé offensant, avec des exceptions flexibles pour les adresses approuvées ; ✓ Ne doit pas copier les e-mails internes vers une autre base de données ou source à des fins d'analyse et l'analyse doit être effectuée sur le serveur Microsoft Exchange lui-même ; ✓ Fournir un agent dédié pour Microsoft Exchange, qui fournit des politiques antivirus, anti-spam, anti-hameçonnage, de filtrage de contenu et de pièces jointes, pour tous les e-mails entrants / sortants / internes ; • L'agent MS Exchange doit : ✓ Être pris en charge sur Microsoft Exchange 2013, 2016 et 2019, y compris toutes les mises à jour cumulatives et les Service Packs, avec une prise en charge native de 64 bits ; ✓ Être capable de détecter les logiciels malveillants avancés dans Adobe PDF, MS Office et d'autres formats de documents à l'aide d'une logique statique et heuristique pour détecter les exploits connus et zero-day ; ✓ Être installé sur les serveurs de boîtes aux lettres, Hub et Edge (le cas échéant) ; ✓ Prendre en charge l'intégration avec le filtre de courrier indésirable MS Outlook et prendre en charge l'action de mise en quarantaine locale avec une option de renvoi manuelle en tant qu'expéditeur d'origine par l'administrateur ; ✓ Rechercher dans les e-mails des liens malveillants dans le corps de l'e-mail et les pièces jointes pour bloquer les attaques de phishing via la réputation de sites Web. • Possibilité d'intégration avec la technologie de sandboxing ; • Intégration avec Microsoft System Center Operations Manager et le filtre de courrier indésirable de Microsoft Outlook ; • Empêcher les modifications de règles non autorisées grâce à un contrôle d'accès fondé sur le rôle ; • Analyse configurable et multithread et limitation du processeur, avec utilisation d'AV Stamp pour éviter les inspections en double ;
Licence/garantie/support	2 ans

2. Installation, configuration et mise en service :

Installation des solutions

Le Titulaire est tenu de livrer et installer, à sa charge, les solutions fournies, objet du présent appel d'offres.

Si des solutions sont reconnues non conformes aux spécifications exigées, celles-ci seront rejetées.

23 NOV. 2021

N.B : Le Titulaire est tenu de fournir tous les accessoires nécessaires au bon fonctionnement des solutions proposées dans le cadre du présent appel d'offres, même dans le cas où ces accessoires n'auraient été explicitement indiqués, ni dans le présent CPS, ni dans l'offre du soumissionnaire. L'ANRT considère que ces accessoires sont inclus dans l'offre de prix. L'attributaire sera invité, le cas échéant, à les livrer et les installer, à sa charge.

Configuration et mise en service

Le Titulaire est tenu d'assurer toutes les opérations de configuration, d'intégration et de mise en service des solutions livrées en vue de disposer d'une plateforme opérationnelle « clé en main ». Il devra assurer notamment les opérations suivantes :

- L'implémentation de l'architecture cible fixée et validée en commun accord avec les équipes de l'ANRT lors de la phase d'ingénierie, avec la prise en charge de toutes les opérations et les configurations nécessaires.
- La réalisation des tests nécessaires pour s'assurer du bon fonctionnement des solutions installées et de toutes leurs composantes.
- L'implémentation du scénario de migration validé en commun accord avec les équipes de l'ANRT lors de la phase d'ingénierie.
- L'intégration de la nouvelle plateforme à l'infrastructure réseaux de l'ANRT.

1. Formation et Transfert de compétences

Le prestataire est tenu de dispenser, dans ses locaux, et pour un groupe de six (06) personnes, les modules de formation, catalogués chez le(s) constructeur(s), des solutions proposées (articles 1,2, 3, 4, 5 et 8), avec support de cours et labs officiels.

Pour les articles 6 et 7, le Prestataire est tenu d'assurer un transfert de compétences au profit des équipes de l'ANRT.

Les modules de formation doivent être animées en français par des formateurs qualifiés et certifiés sur les solutions proposées, permettant aux équipes de l'ANRT d'assurer l'administration et l'exploitation des équipements et des solutions mises en place.
La logistique relative à la formation est à la charge du prestataire (outils de formation, support de formation, ...).

2. Support et Licences

Le soumissionnaire doit proposer le support et licences nécessaires au bon fonctionnement de la solution et des fonctionnalités demandées pour une durée de 2 ans. Ce support intègre 2 ans de support technique (matériel et logiciel) de type 8x5, et ce à partir de chaque date de réception provisoire.

Secrétaire Général

Mohammed HASSI-RAHOU

23 NOV. 2021

TITRE II :

Bordereau des prix-détail estimatif

N° DES PRIX 1	Désignations des prestations (*) 2	Unité de mesure ou de compte 3	Quantité (*) 4	Prix unitaire en....(1) Hors TVA En chiffre		Prix Total Hors TVA	
				P.D en (...) Hors TVA 5	P.L Dirhams Hors TVA 6	P.D en (...) Hors TVA 7=4x5	P.L Dirhams Hors TVA 8 = 4x6
1	Pare-feu frontal	Ensemble	02				
2	Pare-feu dorsal	Ensemble	02				
3	Web Application Firewall	Ensemble	02				
4	Passerelle mail sécurisée	Ensemble	02				
5	Contrôle d'accès au réseau	Ensemble	02				
6	Switch d'étage 48 ports	U	02				
7	Switch à 24 ports	U	02				
8	Equipement pour la gestion de flux Internet	Ensemble	01				
9	Solution de sécurité email pour Microsoft Exchange pour 500 comptes (de base)	F	01				
10	Solution de sécurité email pour Microsoft Exchange pour 250 comptes (additionnels)	F	01				
TOTAUX				**Part en devises ($ ou €) (...) Hors TVA(*)**			
				TVA sur part en devise 20% (**)			
				Part en devise TTC			
				Part locale (PL) HT en dirhams			
				TVA sur part locale en dirhams			
				Part locale TTC en dirhams			

(*) : Seules les désignations et les quantités commandées, livrées et réceptionnées peuvent faire l'objet de facturation par le Titulaire.
Le soumissionnaire ou le groupement soumissionnaire sont invités à se reporter aux dispositions de l'article 3 du présent CPS.

Signatures[3]

A: ....., le .....

Signature et cachet du Concurrent

23 NOV. 2021

3 Lors de la signature du marché, le Maître d'Ouvrage co-signé ce Bordereau des prix-détail estimatif

ANNEXES

Exigences Minimales

N.B : A noter que les tableaux en annexe du CPS, dûment remplis par le soumissionnaire en laissant inchangé les deux premières colonnes, doivent être insérées dans la documentation technique. Lorsque le soumissionnaire omet de remplir une case du tableau, il est considéré que sa proposition est conforme aux exigences du CPS.

23 NOV. 2021

Article N°01 : Pare-feu frontal Nouvelle Génération

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type **(à préciser par le soumissionnaire)**		
Firewall de nouvelle génération offrant les services Statefull Firewall.		
Recommandé sur le dernier rapport NSS-Labs NGFW avec un score supérieur à 95% ou Leader sur l'un des trois derniers rapports Gartner Enterprise Network Firewall.		
Deux (2) boitiers.		
Appliance Rackable 19 pouce 1 RU		
Débit NGFW : Minimum 3 Gbps		
Nombre de connexions simultanées avec inspection : 1 million		
Débit d'inspection TLS : Minimum 450 Mbps		
Débit IPsec VPN 1Gbps		
Chaque boitier doit supporter au minimum 8 ports 1GE RJ45.		
Module Firewalling statefull pour assurer le filtrage et inspection des flux entrants et sortants en IPv4 et IPv6		
Filtrage par id utilisateur et par application		
La solution doit permettre la création de règles de sécurité granulaires à base d'adresse IP/Réseau, nom/groupe d'utilisateur, Service, protocoles, Applications, Domaine, FQDN, Pays/continent et profil d'inspection approfondie…		
Permet la prise en compte de la géolocalisation des connexions sortantes et entrantes dans les règles.		

Déchiffrement et analyse des SSL/TLS entrants et sortants		
Possibilité d'exclure un flux du déchiffrement		
Doté du module d'antimalware afin de traquer en temps réel les virus, vers, chevaux de Troie, Botnet, autres menaces avancées.		
Inspection des protocoles http, https, ssh en mode proxy pour contrôler les paramètres des protocoles L7		
Protection contre les attaques de déni de service		
Support de la détection des scans réseaux		
Protection efficace contre les intrusions par IPS		
Analyse des flux et contenu sur la base des signatures et réputation		
Translation d'adresses NAT, PAT et NAT à base de règles		
Routage statique et dynamique (OSPF, RIP, BGP)		
Gestion de la QoS : priorisation des flux, limitation et réservation de bande passante		
Haute disponibilité en mode Actif/Actif ou Actif/Passif		
Offre VLAN tagging		
Licence (IPS, Antimalware, Control APP) pour 2 ans		
Authentification : Radius, Tacacs+ et Active Directory pour les utilisateurs avec possibilité de couplage avec les solutions d'authentification forte		
La solution doit offrir un management centralisé via une interface d'administration et de reporting unique		
Gestion des sauvegardes et restauration de la configuration		

Centralisation du téléchargement et déploiement des mises à jour des signatures, des correctifs et des patchs		
Support SNMPv3		
Licence/garantie/support : 2 ans		

Article N°02 : Pare-feu dorsal Nouvelle Génération

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type **(à préciser par le soumissionnaire)**		
Firewall Nouvelle Génération, Leader sur l'un des trois derniers rapports Gartner Enterprise Network Firewall ou recommandé dans le dernier rapport NSS Labs NGFW avec une protection supérieure à 95%.		
Firewall de nouvelle génération offrant les services Statefull Firewall		
Deux (2) boitiers au niveau du site principal		
Appliance Rackable 19 pouce 1 RU		
Débit NGFW 5 Gbps.		
Un débit Inspection TLS 3 Gbps		
Un débit VPN IPsec 10 Gbps		
Support de 200 000 nouvelles connexions TCP par seconde ;		
Support de 4 millions de connexions TCP simultanées;		
Permet le stockage en local ou dans l'outil d'administration avec une capacité minimale de 2 disques de 240 Gb SSD		
Doté au minimum de 12 ports réseaux 1GbE RJ45		
Doté au minimum de 2 ports réseaux 10GbE SFP+		
Support la haute disponibilité en mode Actif/Passif et en mode Actif/Actif Clustering ;		
Partage de charge entre les firewalls du cluster		
Module IPS (prévention des intrusions) pour se protéger contre les menaces réseau (vers, chevaux de		

Troie ..). Le module IPS doit aussi apporter une protection contre les menaces réseaux existantes et émergentes, à travers deux mécanismes de détection (par signatures et par anomalies).		
Module Filtrage de contenu pour assurer le contrôle de l'accès interne aux contenus Web indésirables ou illégaux ;		
Filtrage en fonction de l'adresse source, adresse destination, utilisateur, service, protocole, interface d'entrée, Type de Device...		
Identification des applications dans le réseau, détection et protection contre les communications réseau malveillantes et dangereuses.		
Supporte la création des règles de firewall basées sur l'identité de l'utilisateur en plus d'autres critères : Source/Destination, IP/Sous Réseau, Port Source/Dest		
Gestion des plages d'adresses, des groupes d'IPs (machines, réseaux, plages d'adresses), des groupes d'utilisateurs, groupes de services...		
Possibilité de visualiser et de désactiver les règles implicites.		
Possibilité d'appliquer et d'associer des règles QoS aux règles de firewall (ACL) ;		
Possibilité de gestion de la bande passante par application.		
Support du Policy Based Routing		
Supporte de l'IPV6 ;		
Support le VPN IPsec Site to Site, Client to Site et le SSL VPN client to site		

23 NOV. 2021

Routage statique et dynamique (OSPF, RIP, BGP)		
Licence pour 2 ans incluant les services (Contrôle applicatif, IPS, antivirus, antimalware VPN IPSec et SSL) ;		
La solution doit offrir un management centralisé via une interface d'administration et de reporting unique. Gestion centralisée des sauvegardes et restauration des configurations		
Licence/garantie/support : 2 ans		

Article N°03 : Web Application Firewall

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type (**à préciser par le soumissionnaire**)		
Challenger ou leader sur l'un des deux derniers rapports Gartner WAF;		
Deux (2) boitiers.		
Support d'un throughput HTTP/HTTPS d'au moins 2 Gb/s		
Doté d'au moins 4 ports 1 GbE RJ45 avec la fourniture de leur SFP		
Doté d'un espace de stockage d'au moins 400 GB;		
RAM : 16 GB		
Accélération Hardware SSL : 2 000 Transactions par seconde		
Doit être capable de gérer le trafic IPv4 et IPv6		
Support de la Haute disponibilité Actif/passif et Actif/Actif Clustering.		
Support de la répartition de charge Niveau 7		
Offre l'accélération Hardware du flux SSL/TLS		
Protection contre les attaques des applications web comme : OWASP Top 10		
Protection contre le DoS et DDoS applicatif		
Inclure des mécanismes de cryptage des données au niveau de la couche 7 pour protéger les clients contre les logiciels malveillants et les Key Loggers.		
Proposer des mécanismes d'atténuation (Limitation du nombre de requêtes, Blocage de requêtes...).		

Utilisation du moteur d'apprentissage automatique.		
Fournir des templates ou assistant de configuration pour les applications standards.		
Protection FTP et SMTP.		
Nombre d'applications illimité.		
La solution doit être capable de détecter et de contenir les attaques ayant notamment pour objectif de découvrir les vulnérabilités d'un site Web.		
Protection contre le mécanisme d'évasion.		
Protection Antivirale notamment via ICAP.		
Offre la validation de la conformité JSON et XML		
La solution doit disposer de mécanismes d'apprentissage automatique de la structure et des éléments d'une application Web.		
Offre la protection par IP Réputation et IP Géolocalisation		
Supporter la Protection contre les attaques automatisées et détection de botNET		
Licence/garantie/support : 2 ans		

Article N° 04 : Passerelle mail sécurisée

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type **(à préciser par le soumissionnaire)**		
Leader dans le dernier rapport « Gartner Magic Quadrant for Secure Email Gateway »		
Deux Boîtiers physiques en haute disponibilité.		
• Processeurs : 1 x 2.1 GHz, 8 core, 2400 Mhz • Mémoire : 16 GB DDR4 • Disque: 1 TB • Interface réseau : 2 ports 1 GE RJ45 Format appliance 19'' ou 1RU		
Licence pour 500 boites de messagerie La licence doit comporter la protection antivirale, antispam, de protection contre les attaques avancées et filtrage par réputation.		
• Relai SMTP intégré ; • Protection Anti-spam ; • Protection contre les malwares avancés (AMP) • Système de réputation dynamique ; • Protection anti-virale (basé sur signature / zero-hour) ; • Protection anti-phishing ; • Protection contre les attaques ciblées (URL et Pièce-jointe) ; • Protection contre les faux e-mails de notification d'erreur; • Filtrage du contenu des e-mails entrants et sortants : Bloquer (ou modifier) les messages qui contiennent des mots ou expressions		

spécifiques enfreignant une règle de contenu définie ; • Scan en temps réel du protocole SMTP. • Data loss protection (DLP) pour se protéger contre la fuite des données confidentielles par le canal mail ; • Cryptage des emails. • Supporter les protocoles de messagerie SMTP, ESMTP, Secure SMTP sur TLS ; • Règles personnalisables pour scanner les messages et les pièces jointes entrants et sortants; • Détection de macros dans les pièces jointes. • Stratégies flexibles pour cibler les expéditeurs ou les destinataires par entreprise, par groupe ou par individu ; • Gestion des autorisations, filtrage, mise en quarantaine, blocage, notification et reporting ; • Intégration avec LDAP pour la validation des adresses des destinataires ; La solution doit supporter la prise en charge de la remédiation automatique sur les serveurs Exchange 2016/2019 pour les fonctionnalités et actions rétrospectives.		
La solution doit, aussi permettre : • La protection contre les attaques et email frauduleux ; • Une analyse multicritère des messages afin de détecter les courriers indésirables ; • Le filtrage en temps réel du contenu des e-mails ; • Application des règles de filtrage en se basant sur les caractéristiques des pièces jointes, des lexiques, et d'autres identifiants (adresse mail interne/externe...).		

• Le moteur anti-spam doit pouvoir utiliser un moteur pouvant s'appuyer sur plusieurs caractéristiques du message afin de qualifier le message de spam ; • La protection contre les menaces mixtes, virus, chevaux de Troie, vers, programmes espions, Url malveillant, logiciels publicitaires, spam, phishing; • La protection multicouche avec un service de gestion dynamique de la réputation des emails pour bloquer les connexions à partir des adresses IP malveillantes ; • Une détection efficace des menaces, du spam et des attaques ciblées (spear phish, codes malicieux) ; • Une protection contre les virus et les infections à travers : o Une protection antivirus « zero-hour ». o Identifier la disposition d'un fichier (propre, inconnu ou malicieux). o La solution doit être capable de pré-classifier les fichiers afin de juger de leur pertinence à être transmis pour analyse dynamique ou pas. o La solution doit être capable de traker le changement de disposition d'un fichier (un fichier propre ou inconnu qui devient malicieux). o Possibilité de vérifier les URLs dans les pièces jointes • Capacité de pouvoir aussi s'intégrer à un sandboxing. • Une liste noire dynamique bloquant les messages entrants en fonction de l'adresse IP, du domaine ou de l'adresse e-mail ;Une liste blanche définie par l'administrateur (expéditeur, relais, nom de domaine)		

• Le blocage et la mise en quarantaine des messages accompagnés de pièces jointes ou d'URL malveillantes afin qu'elles n'atteignent pas la boîte de réception.		
• Administration aisée par interface graphique en HTTPS ou en ligne de commande via SSH. • Possibilité d'administration à distance. • Configuration flexible des politiques de sécurité. • Mise en place de quarantaines différentes pour (les messages détectés comme spams, les messages infectés pas des virus, les messages mis en quarantaine par un filtre de contenu). • Support des services : LDAP, DNS, NTP, http/https, SSH, FTP, SCP, SNMP Génération automatique des rapports (tableaux de bord) qui sont envoyés automatiquement aux administrateurs.		
Licence/garantie/support : 2 ans		

Article N° 05 : Contrôle d'accès au réseau

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type (**à préciser par le soumissionnaire**)		
Leader dans le dernier rapport Gartner de solutions de contrôle d'accès réseau.		
• Format rackable • CPU 8-core, 2.10 GHz minimum • 32 GB de RAM minimum • 1 Disque Dur SAS de 600 GB minimum Interfaces réseaux nécessaires au déploiement : 4 x 1GBase-T		
Deux Boîtiers physiques en haute disponibilité		
500 clients simultanés.		
• L'authentification de l'utilisateur doit se faire par : o Authentification 802.1X standard o Authentification Web en mode Centralisé o MAB : Mac Address Bypass • La solution doit pouvoir fonctionner comme serveur RADIUS. Elle devra permettre la construction des règles d'authentification et autorisation (politiques) et permettre de configurer des groupes de politiques. • La solution doit distinguer si la requête provient d'un équipement d'accès wifi (RADIUS NAS-Port-Type = Wireless – IEEE 802.11) et si l'authentification est de type 802.1X (RADIUS Service-Type = Framed), MAB (RADIUS Service-Type = Call Check) ou même pour ouvrir une session d'administration Telnet/SSH sur un équipement réseau (RADIUS Service-Type = Login). • La solution devra supporter la liste des protocoles d'authentification suivants : o Host lookup / MAB		

○ PAP / ASCII ○ CHAP ○ MS-CHAPv1, MS-CHAPv2 o EAP-MD5 ○ EAP-TLS ○ EAP-TTLS (depuis la version 2.0) ○ LEAP ○ PEAP (MS-CHAPv2, EAP-TLS et EAP-GTC) ○ EAP-FAST (MS-CHAPv2, EAP-TLS et EAP-GTC) La solution doit permettre la possibilité de faire une authentification double « machine + utilisateur » au sein d'une même authentification (EAP-Chaining)		
La solution devra pouvoir s'appuyer sur sa base interne (équipements ou utilisateurs) ou bien une base externe. La solution devra supporter différents types de base externe : • Ms Active Directory (2016, 2019) • Serveurs LDAPv3 • Serveur Radius Externe • Serveur de certificats d'entreprise SAML pour les portails Web (Oracle Access Manager par exemple)		
Les règles d'autorisation doivent pouvoir être construites en évaluant des conditions. La solution doit avoir le concept de « Policy Sets » permettant de configurer des groupes de politiques d'authentification et d'autorisation, en séparant notamment les règles pour l'accès wifi de celles pour l'accès filaire ou VPN. La solution doit pouvoir intégrer des profils d'équipements réseaux adaptés à différents constructeurs.		
L'accès invité doit être inclus dans la solution. La solution doit disposer de base d'une fonctionnalité Guest complète avec différents portails WEB : • Portail Guest • Portail Sponsor (création des comptes) • Portail BYOD (enregistrement des équipements)		

• Portal Self registration (pour les invités qui veulent créer leur propre compte) • Portail MDM (pour l'interaction avec les MDM) Le renvoi vers un de ces portails est effectué via une URL de redirection qui est envoyée via la solution à un commutateur ou un contrôleur Wireless. L'utilisateur sera automatiquement redirigé vers la page du portail lorsqu'il ouvrira une page web. L'ensemble des pages du portail web doivent être entièrement personnalisables via l'interface de la solution.		
La solution doit supporter les annuaires ci-après, pour la vérification des coordonnées d'un invité à travers le portail captif : Interne : l'annuaire standard où l'administrateur peut créer des utilisateurs à tout moment. Externes : les annuaires MS AD, Radius et LDAP. Guest : un annuaire interne, les utilisateurs étant créés directement par les sponsors ou par les invités eux-mêmes à travers la procédure de self-service qui permet aux invités d'auto-enregistrer leurs noms d'utilisateur et mots de passe. Les utilisateurs doivent pouvoir être authentifiés soit vers les annuaires interne et externe, soit vers l'annuaire Guest, soit vers les trois en spécifiant une séquence d'annuaires à interroger.		
L'utilisation de la base de données locale Guest doit permettre de collecter un certain nombre d'informations sur les invités et de leur assigner un groupe ainsi que des limites horaires de connexion.		
La solution doit supporter la fonction de profiling permettant de classifier les équipements selon les données contenues dans plusieurs types de trafic en fonction de leur provenance.		
A travers différents types d'agents installés au niveau du poste de travail, la solution doit supporter la vérification de plusieurs règles de conformité pour contrôler si un antivirus a été installé,		

si sa version est mise à jour, si certains services ou applications fonctionnent correctement sur le poste de travail, etc. Selon l'état de conformité du poste de travail, il est possible de lui garantir un niveau d'accès spécifique, ou éventuellement lui assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation. Le contrôle de conformité du poste de travail doit porter au minimum sur : • Niveau des patchs des systèmes Microsoft Windows 7, Windows 8, Windows 10. • Contrôle des MAJ des listes des définitions des virus pour les principaux Antivirus. • Contrôles des services non essentiels pour les postes de travail et qui présentent un danger : Service Serveur Web, Serveur FTP et Serveur Telnet. L'administrateur doit pouvoir décider si la remédiation est obligatoire ou optionnelle, manuelle ou automatique.		
• La solution devra fournir un tableau de bord (dashboard) affichant des métriques temps réel des utilisateurs et terminaux connectés au réseau. • La solution doit permettre de générer des rapports en utilisant des modèles prédéfinis et personnalisables. • La solution doit permettre de générer plusieurs types de rapports, notamment sur les performances du système, opérations d'administration, • Authentification Radius… Les rapports doivent être exportables en format CSV ou PDF.		
Licence/garantie/support : 2 ans		

Article N°06 : Switch d'étage à 48 ports

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type **(à préciser par le soumissionnaire)**		
• Châssis Rackable 19"		
• 48 ports 10/100/1000 Mbps PoE+ • 4 ports 1 Gigabit Ethernet SFP		
Performances : • 2 GB de DRAM • 4 Go de Flash • Capacité de commutation d'au moins 100 Gbps (IPv4)		
Support des protocoles Niveau 2, RIPv1, RIPv2, RIPng, OSPF (Accès routé), PBR, PIM Stub Multicast, PVLAN, VRRP		
Support du protocole standard 802.1ae MACSec-128 permettant la sécurisation de la couche MAC.		
SNMP v1, v2c, and v3		
Fonctions d'automatisation NETCONF/YANG, RESTCONF, PnP		
Un bloc d'alimentation avec possibilité d'ajouter un deuxième bloc.		
Licence/garantie/support : 2 ans		

Article N°07 : Switch à 24 ports

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type **(à préciser par le soumissionnaire)**		
• Châssis Rackable 19"		
• 24 ports 10/100/1000 Mbps • 4 ports 1 Gigabit Ethernet SFP		
Performances : • 2 GB de DRAM • 4 Go de Flash • Capacité de commutation d'au moins 50 Gbps (IPv4) • Jusqu'à 3 000 entrées de routage IPv4		
Support des protocoles Niveau 2, RIPv1, RIPv2, RIPng, OSPF (Accès routé), PBR, PIM Stub Multicast, PVLAN, VRRP		
Support du protocole standard 802.1ae MACSec-128 permettant la sécurisation de la couche MAC.		
SNMP v1, v2c, and v3		
Fonctions d'automatisation : NETCONF/YANG, RESTCONF, PnP		
Un bloc d'alimentation avec possibilité d'ajouter un deuxième bloc		
Licence/garantie/support : 2 ans		

Article N° 08 : Equipement pour la gestion de flux Internet

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type (**à préciser par le soumissionnaire**)		
Appliance rackable 19 Pouces		
Performances : • Local Traffic Manager (LTM) • Mémoire: 16 GB • Processeur: 1x deux core Intel Xeon • Débit 10 Gbps L4/L7		
Module DNS (GSLB, DNS, DNSSEC)		
Ports : 4 SFP 1000BASE-T Transceiver		
Un bloc d'alimentation avec possibilité d'ajouter un deuxième bloc.		
Licence/garantie/support : 2 ans		

Article N° 09 : Solution de sécurité email pour Exchange

Spécifications minimales	Proposition du soumissionnaire	Déclaration conformité par soumissionnaire (Oui/Non)
Marque et Type **(à préciser par le soumissionnaire)**		
Leader dans le rapport The Forrester Wave™: Enterprise Email Security, 2021.		
500 comptes.		
• La solution doit : ✓ Utiliser les techniques de détection les plus avancées, y compris l'apprentissage automatique prédictif et la détection des exploitations de documents, pour détecter les menaces inconnues dans les fichiers, les macros et les scripts ; ✓ Détecter et prendre des mesures contre les virus / programmes malveillants, chevaux de Troie et vers ; ✓ Être capable de rechercher et de détruire les e-mails en fonction du sujet, de l'expéditeur ou du destinataire du courrier ; ✓ Bloquer les e-mails avec des URL malveillantes avant la livraison et ré-analyse les URL en temps réel lorsqu'un utilisateur clique dessus ; ✓ Prendre en charge la stratégie (DLP) pour éviter la perte de données et les violations de conformité avec des stratégies pré-prédéfinies, utilisant des mots-clés, des expressions régulières et des identifiants régionaux ; ✓ Fournir des stratégies de pièce jointe pour bloquer les pièces jointes nommées ou bloquer les pièces jointes par vrai type de fichier, extension de fichier ou nom de fichier, avec des règles d'exception intégrées à Active Directory ; ✓ Fournir une règle de filtrage de contenu basée sur des mots clés et des expressions régulières pour		

23 NOV. 2021

filtrer le contenu des messages jugé offensant, avec des exceptions flexibles pour les adresses approuvées ; ✓ Ne doit pas copier les e-mails internes vers une autre base de données ou source à des fins d'analyse et l'analyse doit être effectuée sur le serveur Microsoft Exchange lui-même ; ✓ Fournir un agent dédié pour Microsoft Exchange, qui fournit des politiques antivirus, anti-spam, anti-hameçonnage, de filtrage de contenu et de pièces jointes, pour tous les e-mails entrants / sortants / internes ; • L'agent MS Exchange doit : ✓ Être pris en charge sur Microsoft Exchange 2013, 2016 et 2019, y compris toutes les mises à jour cumulatives et les Service Packs, avec une prise en charge native de 64 bits ; ✓ Être capable de détecter les logiciels malveillants avancés dans Adobe PDF, MS Office et d'autres formats de documents à l'aide d'une logique statique et heuristique pour détecter les exploits connus et zero-day ; ✓ Être installé sur les serveurs de boîtes aux lettres, Hub et Edge (le cas échéant) ; ✓ Prendre en charge l'intégration avec le filtre de courrier indésirable MS Outlook et prendre en charge l'action de mise en quarantaine locale avec une option de renvoi manuelle en tant qu'expéditeur d'origine par l'administrateur ; ✓ Rechercher dans les e-mails des liens malveillants dans le corps de l'e-mail et les pièces jointes pour		

bloquer les attaques de phishing via la réputation de sites Web. • Possibilité d'intégration avec la technologie de sandboxing ; • Intégration avec Microsoft System Center Operations Manager et le filtre de courrier indésirable de Microsoft Outlook ; • Empêcher les modifications de règles non autorisées grâce à un contrôle d'accès fondé sur le rôle ; Analyse configurable et multithread et limitation du processeur, avec utilisation d'AV Stamp pour éviter les inspections en double ;		
Licence/garantie/support : 2 ans