Annexe D

Table des matières

1. Introduction

1.1 À propos

L'objectif premier de la demande de propositions (DP) concernant un outil de capture de paquets complets et d'analyse de sécurité est de remplacer une solution de capture de paquets complets et d'analyse de la sécurité à la fin de son cycle de vie et de soutien (31 mars 2016). Le second objectif de la DP est d'établir une méthode pour étendre la solution à l'ensemble du gouvernement du Canada (GC) au fil du temps. Pour atteindre ces deux objectifs, plusieurs exigences obligatoires et cotées ont été mises en place pour évaluer les soumissions. Ce protocole d'essai servira à vérifier un échantillon d'exigences obligatoires dans le cadre du processus de DP. Seule la proposition retenue sera soumise à ce protocole d'essai; en cas d'échec de l'essai, le soumissionnaire sera automatiquement disqualifié et la soumission admissible suivante sera évaluée.

1.2 Portée du document

Le présent document a été rédigé dans le but de valider les exigences suivantes :

- Exigences obligatoires de la DP : C2O7, C2O8, C2O10, C2O11, C2O12, C2O13, C2O15, C2O16, C2O33, C2O35, C2O38, C2O39, C2O41 et C2O42.
- Les cas d'essai se fonderont sur une solution de moyenne taille.

Hypothèses

Le présent document repose sur les hypothèses suivantes :

- un représentant du fabricant d'équipement d'origine (FEO) sera présent pendant les essais et travaillera avec le personnel d'essai de l'État pour exécuter le protocole d'essai;
- les vérificateurs représentant le FEO ont une connaissance approfondie de tous les composants matériels et logiciels de la solution;
- le représentant du FEO fournira le matériel approprié pour mettre la solution à l'essai; ce matériel devra être placé dans le laboratoire d'essai. Le matériel doit correspondre à ce qui est proposé pour la solution de moyenne taille;
- l'essai se déroulera sur 1 ou 2 jours ouvrables;
- l'État fournira le laboratoire d'essai. Les vérificateurs de l'État connaissent très bien ce laboratoire;
- l'essai sera mené au 101 Goldenrod Driveway, Ottawa (Ontario). Le personnel du FEO et de l'État mènera l'essai sur place;
- toutes les données utilisées dans le cadre de l'essai seront non classifiées.

1.3 Environnement d’essai

Un centre d’essai et de développement non classifié sera utilisé. L’environnement d’essai comprend les composants suivants :

1. Postes de travail. Seront fournis par l’État et serviront à générer le trafic sur le réseau. On utilisera un poste de travail doté de Windows 7. Un poste de travail secondaire également doté de Windows 7 servira à indexer les fichiers et à envoyer des courriels.
2. Serveur des opérateurs du Centre des opérations de sécurité (COS). Sera fourni par l’État et sera un serveur Windows 2012. Au besoin, le logiciel nécessaire pour accéder à la solution sera installé sur la solution. Le serveur sera sur le même réseau local que l’interface de gestion de la solution.
3. Solution. Sera fournie par le FEO. Un câble de cuivre de 1 G reliera la solution à un port SPAN F5. Un espace minimal de stockage pour héberger les cas d’essai est requis, à la discrétion du FEO. Le matériel sera retourné au FEO à la fin de l’essai.
4. F5. Sera fourni par l’État. Placé entre le centre d’essai et de développement et le poste de travail. Le trafic provenant et sortant du poste de travail sera reproduit dans la solution à l’aide de l’écriture miroir.
5. Serveur d’applications. Sera fourni par l’État. Serveur Windows 2012. Permettra d’héberger les applications du serveur.
6. CED. Sera fourni par l’État. Centre d’essai et de développement (CED) national du GC.
7. Pare-feu du CED. Sera fourni par l’État. Utilisation d’un pare-feu à base Intel pour donner un accès Internet au CED.
8. Internet. Des sites publics seront consultés pour effectuer plusieurs des essais.

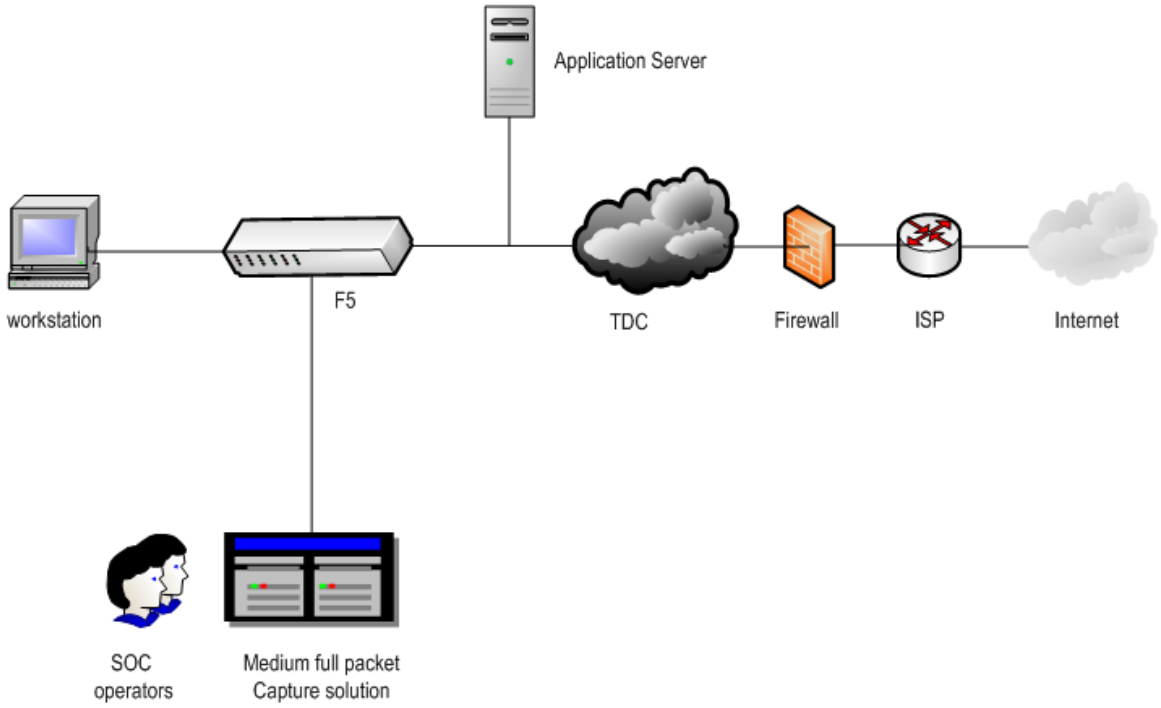

Figure1

Application Server	**Serveur d'applications**
Workstation	**Poste de travail**
F5	**F5**
TDC	**CED**
Firewall	**Pare-feu**
ISP	**FSI**
Internet	**Internet**
SOC operators	**Opérateurs du COS**
Medium full packet Capture solution	**Solution de capture de paquets complets de taille moyenne**

1.4 Éléments ne faisant pas partie de l'essai

Le présent document ne permet pas de soumettre l'infrastructure suivante à un essai :

- le système de gestion central;
- les exigences qui ne sont pas explicitement énumérées à la section 1.2;
- les maliciels connus qui ne seront pas utilisés dans l'environnement d'essai;
- les sites malicieux connus qui ne seront pas consultés dans l'environnement d'essai.

1.5 Terminologie et sigles

Voir l'Énoncé des travaux de la demande de propositions.

2. Protocole d'essai

2.1 Description

La section qui suit vise à documenter les résultats de l'essai et à vérifier un échantillon d'exigences obligatoires de la DP. Les cas d'essai qui ont été créés ne sont pas propres à la solution. L'environnement peut être réglé de façon dynamique selon les besoins d'exécution de chaque cas d'essai. En outre, l'État est libre d'adapter l'exécution de l'essai en fonction de la configuration de l'architecture par défaut du FEO.

2.2 Conditions préalables

Avant l'exécution des cas d'essai, il faut préalablement configurer les composants énumérés à la section 1.4 de la façon suivante :

- Poste de travail secondaire
  - ☐ Installer les applications suivantes : Microsoft Outlook 2010, Microsoft Office 2010, Wireshark, Notepad, Internet Explorer, navigateur Google Chrome, RDP client et FTP client.
  - ☐ Installer le module d'extension PDF d'Adobe Reader sur les navigateurs Internet Explorer et Google Chrome.
  - ☐ Les navigateurs Internet Explorer et Google Chrome sont configurés pour utiliser un proxy Web : 172.16.16.80:8080.
  - ☐ Attribuer une adresse IP statique en 172.16.16.12 avec masque de sous-réseau en/24 et passerelle par défaut en 172.16.16.250.
  - ☐ Créer un fichier Microsoft Word et entrer le texte suivant : « *Le renard brun saute rapidement par dessus le chien paresseux* » et l'enregistrer sous le nom « *test.docx* » sur le bureau.
  - ☐ Ouvrir une session sous « testuser2 », puis ouvrir Microsoft Outlook et envoyer un courriel selon les critères suivants :
    - Expéditeur : testuser2@foo.local

      Destinataire : testuser@foo.local

      Objet : « Test »

      Message : « Testing 1 2 3 »

      Pièce jointe : « test.docx »
- Poste de travail
  - ☐ Installer les applications suivantes : Microsoft Outlook 2010, Microsoft Office 2010, Wireshark, Notepad, Internet Explorer, navigateur Google Chrome, RDP client et FTP client.
  - ☐ Installer le module d'extension PDF d'Adobe Reader sur les navigateurs Internet Explorer et Google Chrome.

- ☐ Les navigateurs Internet Explorer et Google Chrome sont configurés pour utiliser un proxy Web : 172.16.16.80:8080.
- ☐ Attribuer une adresse IP statique en 172.16.16.10 avec masque de sous-réseau en/24 et passerelle par défaut en 172.16.16.250.
- ☐ Créer un fichier Microsoft Word et entrer le texte suivant : « *Voici ma proposition pour consolider les services de TI.* » et l'enregistrer sous le nom « *test2proposal.docx* » sur le bureau.
- ☐ Créer un fichier Microsoft Word et entrer le texte suivant : « *Le renard brun saute rapidement par dessus le chien paresseux* » et l'enregistrer sous le nom « *test.txt* » sur le bureau.

- Solution
  - ☐ Créer les comptes d'essai suivants :
    i. Utilisateur-Admin (administrateur)
    ii. Utilisateur-COS (opérateur COS)
    iii. Utilisateur-invité (invité)
- Serveur des opérateurs du COS
  - ☐ Installer le pupitre de commande de la solution (le cas échéant).
  - ☐ Internet Explorer sera doté du module d'extension PDF d'Adobe Reader.
  - ☐ Créer un fichier de 1 Go alimenté au préalable avec le trafic PCAP et l'enregistrer sous le nom « import.pcap » sur le bureau.
- Serveur d'applications
  - ☐ Serveur DNS de Windows configuré avec le domaine foo.local
  - ☐ Site FTP avec au moins un dossier dans le répertoire racine
  - ☐ Créer une sous-page de foo.local : http://www.foo.local/bigpage.html
    i. Configurer à l'aide de la compression GZIP de niveau 6 (http://www.iis.net/configreference/system.webserver/httpcompression/scheme).
  - ☐ Microsoft Exchange configuré en tant que serveur SMTP comptant les comptes de courriels d'essai suivants :
    i. testuser@foo.local
    ii. testuser2@foo.local
    iii. testuser3@foo.local

Remarques :

1. Le compte de l'opérateur du COS (« Utilisateur-COS ») sera toujours utilisé pour valider les cas d'essai sur le pupitre de commande de la solution, à moins d'indication contraire.
2. Le compte « testuser » sera toujours utilisé pour ouvrir une session sur le poste de travail afin d'exécuter les cas d'essai, à moins d'indication contraire.

2.3 Cas d'essai

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
1.	C2O7. La solution doit pouvoir fonctionner dans un déploiement hors bande consistant en un TAP réseau ou un commutateur par paquets qui reproduit le trafic du réseau dans la solution.	1. Ouvrir une session dans le poste de travail et lancer Wireshark. 2. Commencer la capture en direct à l'aide d'un filtre sur le trafic HTTP. 3. Ouvrir le navigateur Internet Explorer et aller à http://www.canada.ca/en/index.html 4. Une fois la page entièrement téléchargée, arrêter la capture en direct sur Wireshark. 5. Se connecter au serveur des opérateurs du COS. 6. Dans la solution, aller à la visualisation des données brutes et filtrer le trafic HTTP.	L'opérateur du COS choisit au hasard un échantillon de 10 paquets. L'échantillon doit correspondre aux données de Wireshark dans la solution.		
2.	C2O8. La solution doit prendre en charge le contrôle d'accès basé sur les rôles. À tout le moins, les rôles suivants sont obligatoires :	1. Se connecter au serveur des opérateurs du COS. 2. Ouvrir une session dans la solution sous Utilisateur-Admin. 3. Vérifier les privilèges du compte. 4. Sortir du compte Utilisateur-	• L'utilisateur-Admin doit pouvoir créer, lire, mettre à jour et supprimer tous les aspects de la		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE / ÉCHEC
	• Administrateur • Opérateur • Invité	Admin. 5. Se connecter au compte Utilisateur-COS. 6. Vérifier les privilèges du compte. 7. Sortir du compte Utilisateur-COS. 8. Se connecter au compte Utilisateur-invité. 9. Vérifier les privilèges du compte. 10. Sortir du compte Utilisateur-invité.	solution. • L'utilisateur-COS doit pouvoir interroger des paquets et générer des rapports. • L'utilisateur-invité doit seulement pouvoir voir certains aspects de la solution.		
3.	C2O10. La solution doit pouvoir prendre en charge l'analyse ou le décodage et la reconstruction des couches d'application 4 à 7 des protocoles suivants : • (3a) serveur DNS à serveur interne; • (3b) serveur FTP à serveur interne.	**3a :** 1. Ouvrir une session dans le poste de travail. 2. Lancer une invite de commande et effectuer les commandes suivantes : a. nslookup www.foo.local (serveur ip) b. nslookup – type=mx foo.local (serveur IP) c. nslookup –type=ns foo.local (serveur IP) 3. Noter les résultats des commandes.	• 3a : Dans la solution, vérifier que les commandes DNS sont correctement reconstruites. • 3b : Dans la solution, la session reconstruite doit s'afficher correctement; il faut aussi être capable de voir les commandes « dir » et « cd		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
		4. Se connecter au serveur des opérateurs du COS. 5. Dans la solution, reconstruire le trafic du serveur DNS. **3b :** 6. Ouvrir une session dans le poste de travail. 7. Lancer une session FTP dans le serveur d'applications. 8. Une fois la session FTP ouverte, entrer les commandes suivantes : a. dir b. cd switch folder 9. Fermer la session FTP. 10. Se connecter au serveur des opérateurs du COS. 11. Dans la solution, reconstruire le trafic du serveur FTP.	switch folder ».		
4.	C2O11. La solution doit pouvoir appliquer les filtres BPF (Berkeley Packet Filters) pour cibler les paquets échangés devant être captés ou ignorés.	1. Se connecter au serveur des opérateurs du COS. 2. Activer les filtres BPF dans la solution et appliquer les filtres suivants : a. permettre les paquets HTTP;	La solution ne doit que capturer les paquets HTTP sortants. Les paquets HTTPS ne sont pas présents.		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
		b. ignorer le port source 443. 3. Se connecter au poste de travail, ouvrir le navigateur Internet Explorer et aller aux sites Web suivants : a. https://www1.bmo.com/onlinebanking/cgi-bin/netbnx/NBmain?product=5 ; b. http://www.canada.ca/ 1. Se connecter au serveur des opérateurs du COS. 2. Dans la solution, vérifier le trafic capturé.			
5.	C2O12, C2O33. La solution proposée doit offrir des capacités de recherche de données pour soutenir les expertises judiciaires en réseaux et le traitement des incidents. Toutes les demandes/recherches de données ou l'indexage par méta-données doivent pouvoir se faire en 120 secondes par une	1. Se connecter au poste de travail, ouvrir le navigateur Internet Explorer et aller aux sites Web suivants : a. http://www.canada.ca/en.html ; b. http://www.canada.ca/en/contact.html ; c. http://www.canada.ca/en/government/system.html ; d. http://open.canada.ca/en?_ga=1.161942908.19086488	Dans l'IUG de la solution : • 10a : Les résultats doivent seulement contenir des courriels IE avec « canada » dans le message • 10b : Les résultats contiennent des agents d'utilisateur IE et		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE / ÉCHEC
	recherche dans toutes les données recueillies au cours de la journée précédant la recherche. Remarque : L'exigence d'essai a été révisée en fonction d'une journée de conservation. L'exigence obligatoire de la DP concernant la période de conservation n'est pas possible puisque l'essai est mené sur 1 ou 2 jours.	2.1449089745 2. Ouvrir le navigateur Chrome puis aller aux sites Web suivants : a. http://www.canada.ca/en.html ; b. http://www.canada.ca/en/contact.html ; c. http://www.canada.ca/en/government/system.html ; d. http://open.canada.ca/en?_ga=1.161942908.1908648822.1449089745 3. Ouvrir Windows Outlook puis créer et envoyer les courriels suivants : a. Courriel 1 *Destinataire : testuser2@foo.local* *Objet : « Allo le monde »* *Message : « Avez-vous reçu ma proposition de projet ? Elle est attendue la semaine prochaine. »* *Pièce jointe :*	Chrome avec « canada.ca » dans l'URL • 10c : Les résultats ne doivent que retourner le trafic de Chrome • 10d : Un (1) résultat du courriel 1 • 10e : Un (1) résultat du courriel 1 • 10f : Un (1) résultat du courriel 3 • 10g : Au moins 3 résultats des courriels 1, 2 et 3. Peut également comporter des résultats provenant des cas d'essais précédents. • 10h : Les résultats ne		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE / ÉCHEC
		« test.docx » b. Courriel 2 *Destinataire : testuser3@foo.local* *Objet : « Lundi matin »* *Message : « Travaillons à notre proposition de projet. Nous devons la terminer cette semaine. »* *Pièce jointe : « test2proposal.docx »* c. Courriel 3 *Heure : » Envoyer une demi-heure après les courriels 1 et 2* *Destinataire(s) : testuser1@foo.local ; testuser2@foo.local* *Objet : « Planification stratégique »* *Message : « La pièce jointe est terminée. À revoir. J.ai eu l'aide de Jake. Son courriel est Jake@foo.local »* *Pièce jointe :*	contiennent que le trafic de l'adresse source IP « 172.16.16.x » • 10 i : Les résultats ne contiennent que le trafic des ports sources 443 et 7016		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE / ÉCHEC
		« test2proposal.docx » 4. Se connecter au serveur des opérateurs du COS. 5. Dans la solution, faire les recherches suivantes : a. (10a) Page Web contenant « *canada* » ET agent d'utilisateur = Internet Explorer b. (10b) URL contenant « *canada.ca* » c. (10c) Tout trafic n'employant pas Internet Explorer comme agent d'utilisateur d. (10d) Objet = « *Allo le monde* » e. (10e) Destinataire = testuser2@foo.local ET message contenant « *proposition* » f. (10f) Échéance dans la dernière demi-heure ET titre de pièce jointe contenant « *tes*.doc* » g. (10g) Recherche approximative de			

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
		« *@foo.local » h. (10h) IP source contenant « *172.16.16.x* » i. (10i) Ports sources contenant 443, 7016			
6.	C2O13. La solution doit offrir des capacités d'exportation et d'importation de données à l'aide du format PCAP.	1. Ouvrir une session dans le poste de travail, ouvrir le navigateur IE et aller aux pages Web lourdes de la bande passante. 2. Se connecter au serveur des opérateurs du COS. 3. Dans la solution, exporter les dix derniers Go de capture de trafic brute en format PCAP et les enregistrer sur le bureau sous le nom « export.pcap ». 4. Importer les données de « import.pcap » dans la solution.	• La solution peut importer « import.pcap » avec succès. • La solution peut exporter dix Go de trafic brut avec succès. • Le fichier « export.pcap » peut être importé et lu dans Wireshark.		
7.	C2O15. La solution doit pouvoir décoder le trafic compressé selon un code de contenu HTTP au niveau du trafic Web (couche d'application) à partir du système de compression suivant, notamment GZIP selon l'algorithme DEFLATE.	1. Ouvrir une session dans le poste de travail, ouvrir le navigateur IE et aller à http://www.foo.local/bigpage.html. 2. Se connecter au serveur des opérateurs du COS. 3. Dans la solution, mettre à l'essai la reconstruction de la page Web	L'IUG de la solution doit pouvoir reconstruire la page Web compressée et l'afficher dans un format lisible par l'utilisateur.		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
	Par exemple : Serveur Web compressant le code HTML au navigateur Web	compressée.			
8.	C2O16. La solution doit fournir un service de renseignement contre les menaces au réseau qui est mis à niveau pour le fournisseur au moins une fois par semaine (voir l'EDT pour tous les détails). Le service de renseignement doit à tout le moins pouvoir : • détecter le trafic en provenance ou à destination de serveurs Web soupçonnés d'être infectés (en fonction de l'URL ou de l'IP); • détecter le trafic en provenance ou à destination de points de sortie TOR; • détecter le trafic en provenance de	1. S'assurer de désactiver la configuration du proxy. 2. Ouvrir une session dans le poste de travail, ouvrir le navigateur IE et aller à un point de sortie TOR connu via https. Valider à partir de la date d'essai et comme convenu entre les vérificateurs du FEO et de l'État. 3. Se connecter au serveur des opérateurs du COS. 4. Dans la solution, vérifier le trafic.	L'IUG de la solution devrait automatiquement détecter la destination en tant que TOR.		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
	maliciels connus.				
9.	C2O35. Pour la reconstruction de sessions de réseau qui contiennent des données texte, le processus de reconstruction doit être compatible avec les réglages d'affichage des caractères Unicode et pouvoir les afficher. La solution doit être compatible avec les langues alphabétiques et logogrammiques et pouvoir afficher le texte reconstruit dans la langue qui s'y rattache. À tout le moins, les sessions de réseau contenant les langues suivantes doivent être décodées par la solution : • Anglais • Mandarin	1. Ouvrir une session dans le poste de travail, ouvrir le navigateur IE et aller à http://chinese.korea.net/index.jsp. 2. Une fois la page entièrement téléchargée, se connecter au serveur des opérateurs du COS. 3. Dans la solution, reconstruire le trafic.	Dans l'IUG de la solution, le trafic reconstruit doit être semblable au site qui est directement affiché dans un navigateur. La langue et la mise en page doivent s'afficher correctement.		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
10.	C2O38. La solution peut associer toutes les adresses IP sources et les adresses IP de destination à un emplacement géographique du pays.	1. Se connecter au poste de travail, ouvrir le navigateur Internet Explorer et aller aux quatre sites Web suivants : a. http://www.apnic.net (Asie); b. http://www.enisa.europa.eu (Europe); c. http://www.afrinic.net (Afrique); d. http://www.google.com (Amérique du Nord). 2. Une fois tous les sites Web téléchargés, se connecter au serveur des opérateurs du COS. 3. Dans la solution, localiser le trafic et cerner l'emplacement géographique de chaque adresse IP.	L'IUG de la solution devrait indiquer correctement l'information géographique des sites Web.		
11.	C2O39. La solution doit pouvoir ajouter une étiquette descriptive personnalisée aux adresses IP internes privées.	3. Se connecter au serveur des opérateurs du COS. Dans la solution, attribuer l'étiquette « Boîte du labo » à l'adresse IP du poste de travail. 4. Ouvrir une session dans le poste de travail, ouvrir le navigateur IE et aller à www.google.com	L'IUG de la solution devrait afficher l'étiquette de l'adresse IP du poste de travail comme étant la « Boîte du labo ».		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE / ÉCHEC
		5. Se connecter au serveur des opérateurs du COS. 6. Dans la solution, localiser le trafic interne et vérifier l'étiquette.			
12.	C2O41. La solution doit pouvoir reconstruire et afficher toute la page Web dans le cadre de la reconstruction de la session (à l'exception du contenu encrypté).	1. Se connecter au poste de travail, ouvrir le navigateur Internet Explorer et aller aux sites Web suivants : a. http://www.cra-arc.gc.ca/E/pbg/tf/rc66/README.html; b. http://www.cra-arc.gc.ca/E/pbg/tf/rc66/rc66-15e.pdf 2. Une fois les deux pages entièrement téléchargées, se connecter au serveur des opérateurs du COS. 3. Dans la solution, reconstruire les sessions et afficher les pages Web. Remarque : Si les URL ne sont plus actifs au moment de l'essai, ils peuvent être remplacés par des adresses comparables.	• L'opérateur du COS devrait pouvoir visualiser les pages Web reconstruites en format *.HTML* à partir du pupitre de commandes de la solution. • L'opérateur du COS devrait pouvoir visualiser le fichier *PDF* reconstruit à partir du pupitre de commandes de la solution. Le contenu devrait correspondre à celui des pages Web affichées sur le poste de travail.		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
13.	C2O42. La solution doit pouvoir reconstruire des fichiers à partir du trafic capturé et permettre de les télécharger. À tout le moins, les fichiers suivants doivent pouvoir être reconstruits : • (5a) fichiers joints aux courriels SMTP; • (5b) fichiers transférés à l'aide du serveur FTP.	**5a :** 1. Ouvrir une session dans le poste de travail. 2. Lancer Microsoft Mail et veiller à ce que la boîte de réception soit à jour en cliquant sur le bouton « Envoyer/recevoir ». 3. Confirmer que le courriel provenant de testuser2@foo.local a été reçu avec pièce jointe. 4. Se connecter au serveur des opérateurs du COS. 5. Dans la solution, reconstruire la session SMTP et télécharger le message du courriel. **5b :** 1. Ouvrir une session dans le poste de travail. 2. Lancer une session FTP dans le serveur d'applications. 3. Une fois la session FTP session lancée, transférer le fichier « test.txt » dans le répertoire du serveur d'applications à l'aide de la commande « put ». 4. Fermer la session FTP.	• 5a : Dans la solution, l'opérateur du COS devrait pouvoir reconstruire la session SMTP, visualiser le contenu du courriel et ouvrir le document Word. Le contenu devrait correspondre à celui du scénario d'essai. • 5b : Dans la solution, l'opérateur du COS doit pouvoir reconstruire la session FTP et ouvrir le fichier texte. Le contenu devrait correspondre à celui du scénario d'essai.		

N° de cas	Description	Exécution de l'essai	Résultat souhaité	Résultat réel	RÉUSSITE /ÉCHEC
		5. Se connecter au serveur des opérateurs du COS. 6. Dans la solution, reconstruire la session FTP et télécharger le fichier « test.txt ».			