

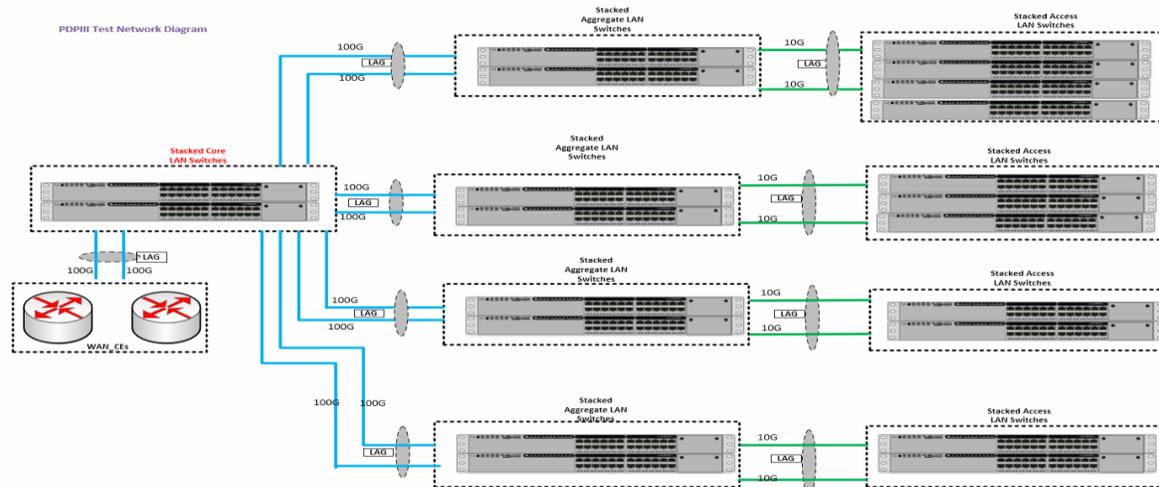
## Annexe D - Plan de test d'intégration

Tous les tests seront effectués sur place dans la région de la capitale nationale en utilisant des configurations de production, sauf indication contraire. Le fournisseur, avec le soutien de Services partagés Canada (SPC), connectera deux commutateur principal de couche 3, deux commutateur d'agrégation et trois commutateurs d'accès, deux multigigabit et un gigabit par pile, selon le schéma ci-dessous. SPC fournira des conseils de configuration appropriés, comme c'est le cas actuellement en production pour SPC, afin de faciliter les essais.

Les configurations logicielles mises en place pour les tests ne peuvent pas être retirées du bâtiment, que ce soit sous forme papier ou électronique. Si les commutateurs de test ne sont pas laissés dans le cadre de la livraison de l'équipement principal (dans l'hypothèse d'un résultat positif), les configurations doivent être réinitialisées aux valeurs par défaut avant de quitter le laboratoire.

Exigences minimales relatives à l'équipement du banc d'essai	Quantité
Configuration de commutateur principal de couche 3	2
Configuration de commutateur d'agrégation	2
Configuration de commutateur d'accès multigigabit	4
Configuration de commutateur d'accès gigabit	2
Câble de cascade supplémentaire pour items 3 et 4 - 1 mètre	2
Émetteur-récepteur 10GBASE-LR	8
Émetteur-récepteur 10GBASE-SR	8
Émetteur-récepteur 100GBASE-SR-BiDi	8

Plus tous les câbles d'empilage, cordons d'alimentation, ventilateurs et alimentations nécessaires pour répondre aux exigences de l'annexe C.



- Test 1 Automatisation du réseau local (accès, agrégation et principal de couche 3)**  
Le fournisseur doit faire la démonstration de Zero-Touch Provisioning (ZTP), du push de configuration, des changements de configuration, du renouvellement de licence, de la mise à niveau du logiciel d'exploitation et de la mise à niveau en service sans aucune interruption de service.
- Test 2 Le fournisseur doit démontrer la résilience (accès, agrégation et principal de couche 3)**  
Un dispositif est branché sur le commutateur d'accès sur un vlan donné émulant un utilisateur, un autre dispositif est également branché sur le noyau, les deux dispositifs doivent être sur le même réseau en utilisant la même ID Vlan. Un ping continu est initié entre le dispositif central et le dispositif utilisateur. Le fournisseur devra éteindre l'unité de pile transportant le trafic ICMP et démontrer que le trafic est récupéré sans perte de paquets ou avec un maximum de 3 pertes de paquets.
- Test 3 Paquets provenant de l'interface de gestion Inband au sein d'un VRF sur le commutateur principal de couche 3.**  
Le fournisseur doit démontrer que le trafic de gestion peut provenir d'une interface de gestion en bande dans un VRF sur le routeur central. Le trafic de gestion, tel que NTP, Syslog, SNMPv3, SSH, TACACS+, etc.
- Test 4 Le fournisseur doit démontrer l'existence de la norme 802.1x (NAC sur les commutateurs d'accès uniquement, support de EAP-TLS en MAC bypass).**  
Le fournisseur doit démontrer la fonctionnalité 802.1x et l'interopérabilité avec la solution Aruba Clearpass.  
Le fournisseur doit démontrer que le commutateur d'accès est capable d'analyser et de traiter les attributs RADIUS suivants qu'il reçoit de la réponse RADIUS (ACCEPT, DROP, REJECT) :
- Attribut 81 : Tunnel-Private-Group-Id tel que défini dans RFC2868. Le commutateur doit être capable de définir le VLAN sur la base d'un ID VLAN numérique (exemple VLAN '63') ou d'une étiquette VLAN (exemple VLAN 'Corporate').
  - Attribut 92 : NAS-Filter-Rule tel que défini dans la RFC4849 et/ou Attribut 11 Filter-id. Si l'attribut 92 est utilisé, le commutateur doit définir un ACL basé sur la valeur de la chaîne envoyée par l'attribut du serveur RADIUS. Si l'on utilise l'attribut 11 filter-id, l'ACL doit être préconfiguré sur le commutateur et activé sur le port si le nom de l'ACL est transmis par la réponse RADIUS 11.
  - Le port Dot.1x doit prendre en charge la VoIP afin de garantir qu'un ensemble de téléphones est placé dynamiquement sur un Vlan donné et que le même port Dot1x est capable de prendre en charge un dispositif branché en série avec le téléphone VoIP et que le dispositif est également placé dynamiquement sur un VLAN différent de celui de l'ensemble de téléphones.

- Test 5**      **Le vendeur doit démontrer l'isolation du trafic (Principal de couche 3)**  
Test effectué hors ligne avec une construction provisoire complète de niveau 1 (Principal de couche 3).  
Virtual Route Forwarding (VRF) doit être configuré sur le commutateur principal de couche 3 et un VLAN ajouté avec une adresse non-OZ. Si nécessaire, un port peut être activé pour apporter le VLAN ou il peut être activé manuellement si la fonction est disponible. Le trafic du réseau OZ ne doit pas pouvoir atteindre le trafic transporté par le VRF. Le succès sera indiqué par l'isolation du trafic entre les zones (comme indiqué par ping), l'échec sera indiqué par la traversée réussie du vlan indépendamment du VRF.
- Test 6**      **Le fournisseur doit démontrer l'authentification, l'autorisation et la comptabilité de l'utilisateur TACACS+ (Accès)**  
Test effectué en ligne avec des commutateur principal de couche 3 Cisco de SPC  
Le test doit démontrer la réussite de l'accès utilisateur pour l'accès RW et RO via les informations d'identification Active Directory (AD) fournies  
Le test doit démontrer que les niveaux RW et RO tels qu'attribués dans AD sont transmis au commutateur, limitant ou autorisant l'accès aux commandes à privilèges élevés. Les commandes à privilèges élevés seront déterminées au cours de l'évaluation, mais incluent généralement la capacité de modifier et de valider de façon permanente tout élément de configuration non transitif important  
Les tests doivent démontrer la journalisation des sessions SSH/Telnet (lorsqu'un utilisateur tente de se connecter ou se connecte avec succès au commutateur) sur le serveur TACACS+, ainsi que la journalisation des commandes exécutées et du compte utilisateur à partir duquel elles ont été exécutées (également sur le serveur TACACS+)  
L'échec est indiqué par l'impossibilité d'accéder aux commutateurs via TACACS+, par l'impossibilité de séparer les niveaux d'utilisateurs, c'est-à-dire uniquement RW, ou par le fait que ces niveaux de privilèges ne sont pas respectés par le commutateur, c'est-à-dire que les utilisateurs RO se voient accorder des privilèges élevés. L'échec est également indiqué par l'impossibilité d'enregistrer les sessions SSH/Telnet ou les commandes via la comptabilité TACACS+
- Test 7**      **Le fournisseur doit démontrer sa compatibilité avec le système téléphonique VoIP (Access)**  
Les tests doivent démontrer la négociation réussie du POE et la communication de LLDP-MED pour placer le téléphone dans le VLAN vocal correct. Des conseils de configuration seront fournis par le SSC pour s'adapter aux déclarations de configuration du fournisseur. Un test réussi sera indiqué par un combiné VOIP en ligne. L'échec sera indiqué par l'absence de livraison de POE ou l'impossibilité de détecter le VLAN vocal correct via LLDP-MED
- Test 8**      **Le fournisseur doit démontrer que MACsec utilise une clé de 256 bits entre les commutateurs d'accès, d'agrégation et principal de couche 3**  
MACsec doit être configuré entre les commutateurs d'accès, d'agrégation et principal de couche 3. La connectivité entre les commutateurs se fait sur un LAG avec un minimum de deux ports par LAG. Le trafic doit être poussé à plein débit. La mise en miroir des ports doit être activée pour capturer ce trafic et confirmer que le trafic est crypté. Pendant que le trafic traverse, un port dans le lag doit être déconnecté et confirmer que le trafic continue à traverser le lien existant sans perte de paquets ou avec un maximum de 5 pertes de paquets
- Test 9**      **Le fournisseur doit démontrer que l'ajout d'un port au LAG n'a aucun impact sur le trafic existant**  
Pendant que le trafic circule sur le LAG existant, le fournisseur doit ajouter un autre port au LAG et démontrer que le trafic existant continue de circuler sans interruption et sans perte de paquets
- Test 10**      **Le fournisseur doit démontrer que l'ajout et le retrait de l'alimentation électrique d'un commutateur dans la pile n'a pas d'impact sur le flux de trafic**  
Pendant que le trafic circule entre le commutateur principal de couche 3, l'agrégation et l'accès, le fournisseur doit retirer une alimentation électrique d'un commutateur de la pile et démontrer que le trafic n'est pas affecté. La deuxième partie consiste à démontrer que le fournisseur ajoute une alimentation à un commutateur de la pile et s'assure que le trafic n'est pas non plus affecté
- Test 11**      **Le fournisseur doit démontrer la fonctionnalité de RadSec en utilisant un certificat basé sur TLS et l'intégration avec Aruba Clearpass**  
Le commutateur et le serveur RADIUS seront configurés pour communiquer par RADSec à l'aide d'un certificat basé sur TLS. Toutes les autres méthodes seront désactivées pour le serveur RADIUS. S'assurer que la communication entre les commutateurs LAN et le radius (Clearpass) est établie et stable. Répétez le cas de test # 4
- Test 12**      **Le fournisseur doit démontrer l'empilement de commutateurs d'accès gigabit et multigigabit**  
À l'aide de câbles d'empilage, le fournisseur doit démontrer la création réussie d'une pile de commutateurs d'accès composée de deux commutateurs multigigabit et d'un commutateur gigabit