

# Cybersécurité – Gouvernement de l'Î.-P.-É. Mise en œuvre d'un système de prévention d'intrusion



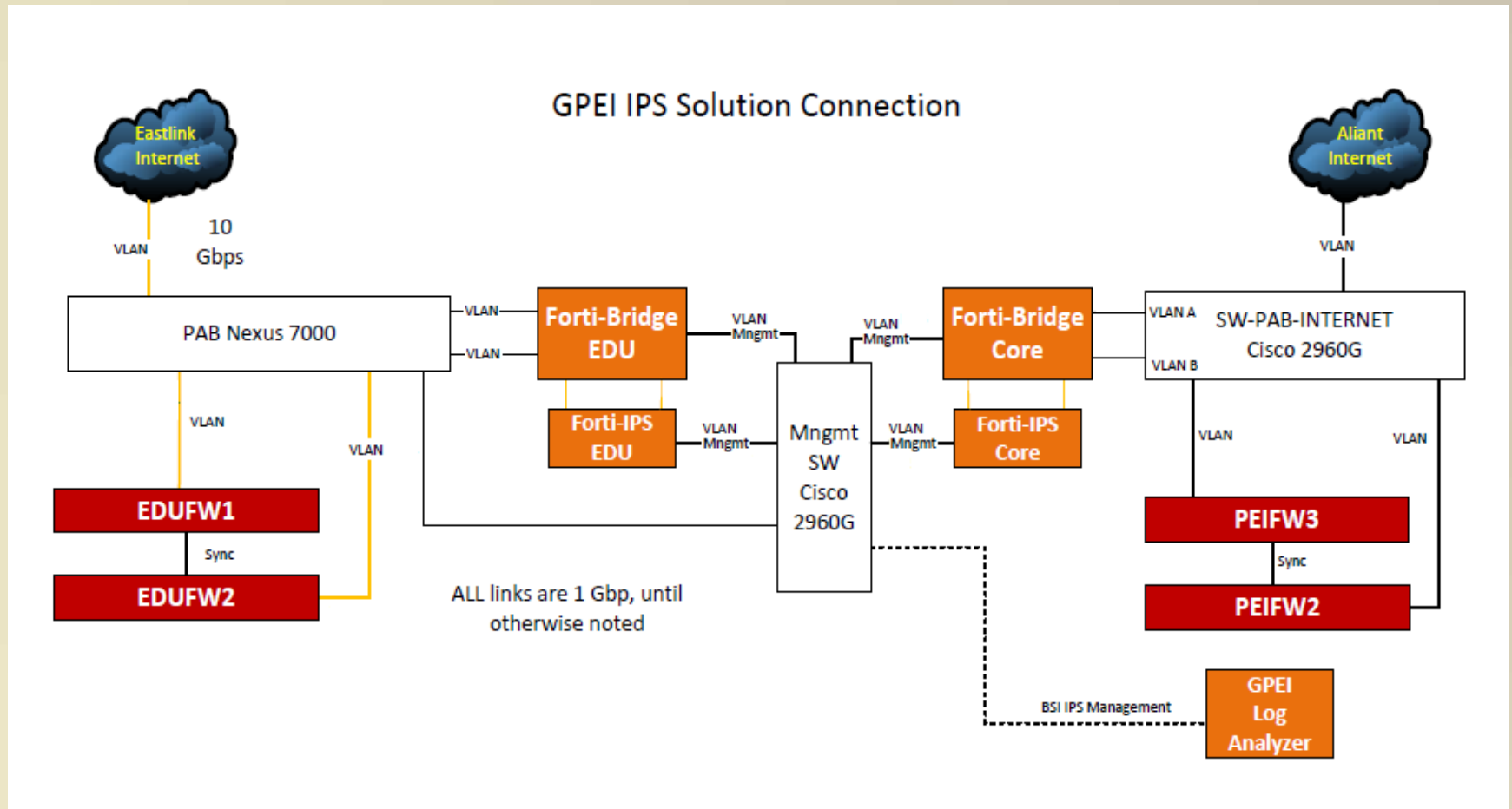
# Réseau du gouvernement

- Plus de 10 000 postes de travail munis de Windows
- 750 serveurs Windows et Linux
- Trois réseaux protégés par des pare-feu – réseau central, réseau santé et réseau éducation


# Historique du système de prévention d'intrusion (IPS)

- Présentation en 2014 d'un tableau de bord au nouvel administrateur en chef des opérations
- Appui suscité auprès de la haute direction
- Notre préférence est accordée à un service géré
- Discussions avec le secteur privé pour déterminer les coûts appropriés
- Demande de fonds déposée
- Demande de propositions (DP) visant un Centre des opérations de sécurité (COS) et un Centre des opérations de réseau (COR)
- Un seul fournisseur a répondu à la DP

# Conception de l'IPS




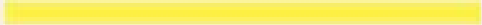










# Processus de mise au point

- Accorder au moins deux semaines
  - Déterminer quels sont les systèmes qui communiquent avec des sources externes
  - Utiliser les règles de pare-feu existantes
  - Effectuer une vérification auprès de la communauté des utilisateurs
- 

# Avantages

## Intrusion Sources


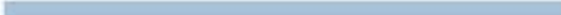










#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	104.237.202.7				72,351	14.73%
2	191.96.249.238				66,439	13.52%
3	211.137.82.38				47,828	9.73%
4	74.81.85.145				47,433	9.65%
5	95.110.174.107				24,333	4.95%
6	185.165.29.103				24,121	4.91%
7	191.96.249.18				24,113	4.91%
8	191.96.249.205				23,796	4.84%
9	220.119.112.241				15,360	3.13%
10	14.38.137.46				14,902	3.03%
11	184.105.247.207				13,495	2.75%
12	184.105.247.199				13,362	2.72%

# Avantages

## GPEI WEEKLY IPS REPORT - Core

FORTINET

### Intrusions Blocked

#	Intrusion Name	Intrusion Type	Severity	Counts
1	 Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Improper Authentication	Critical	 68,624
2	 VxWorks.WDB.Agent.Debug.Service.Code.Execution	Permission/Privilege/Access Control	Critical	 48,601
3	 ASUS.Router.infosvr.UDP.Broadcast.Command.Execution	OS Command Injection	Critical	 24,332
4	 Apache.Struts.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	 243
5	 Joomla.Core.Session.Remote.Code.Execution	Code Injection	Critical	 94
6	 OpenSSL.Heartbleed.Attack	Information Disclosure	Critical	 93

# Leçons apprises

- Participation
- Expertise du fournisseur (expérience et produit)
- Compatibilité entre les réseaux et l'IPS
- Plan de reprise
- Processus de communication avec le fournisseur
- Communication et consultation avec les utilisateurs



# Situation actuelle

- Un problème de compatibilité a forcé le retour du système au mode de surveillance
- Élaborer un plan pour commencer le blocage vers la fin d'octobre (à la lumière de la consultation auprès de la communauté de clients)
- Le réseau de santé provincial sera le dernier à être mis en œuvre

Des questions?

