


Government of P.E.I. Cyber Security Implementing an Intrusion Prevention System



Government Network

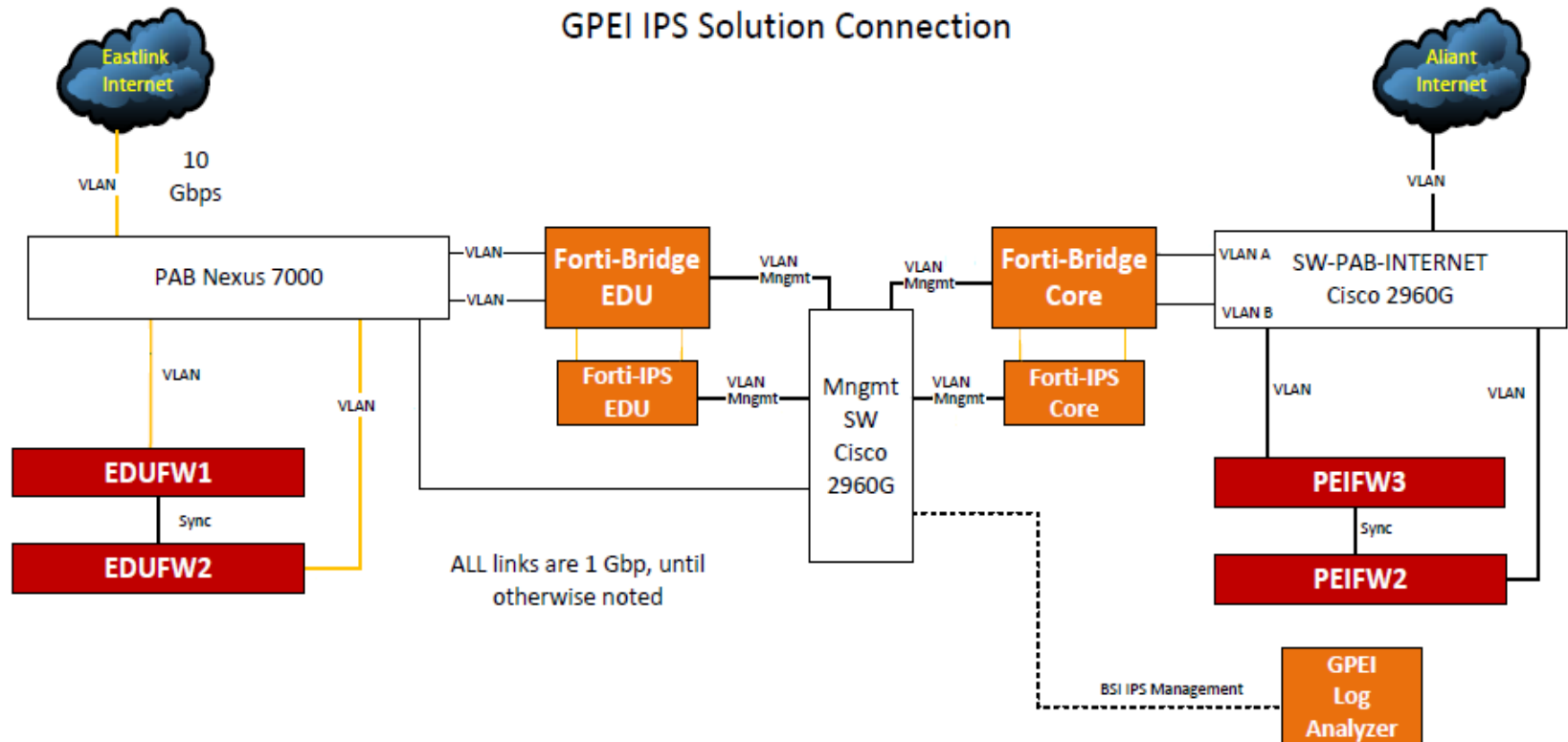
- 10,000+ Windows based workstations
- 750 servers Windows server/Linux
- 3 networks separated via firewalls – Core, Health and Education

IPS Path


- Started in 2014 with a dashboard presentation to incoming COO
 - Built support at senior management level
 - Determined that a managed service was our preference
 - Held discussions with private sector to determine appropriate costs
 - Submitted capital request
 - Issued RFP for a Security Operations Centre (SOC) and a Network Operations Centre (NOC)
 - Only one vendor response received
- 

IPS Design

GPEI IPS Solution Connection













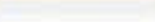




Tuning Process

- Allow at least 2 weeks
 - Determine which systems communicate with external sources
 - Use existing firewall rules
 - Check with user community
- 

Benefits

Intrusion Sources


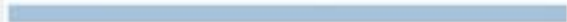



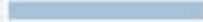






#	Attack Source	Counts	 Critical  High  Medium	Percent of Total Attacks
1	104.237.202.7		72,351	14.73%
2	191.96.249.238		66,439	13.52%
3	211.137.82.38		47,828	9.73%
4	74.81.85.145		47,433	9.65%
5	95.110.174.107		24,333	4.95%
6	185.165.29.103		24,121	4.91%
7	191.96.249.18		24,113	4.91%
8	191.96.249.205		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%

Benefits

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

Lessons Learned

- Involvement
- Vendor expertise (experience and product)
- Compatibility between network and IPS
- Back out plan
- Communication processes with vendor
- Communication/consultation with users

Current State

- Compatibility issue forced system back to monitor mode
 - Plan to start blocking in late October (based on consultations with client community)
 - Final implementation will be the Provincial Health Network
- 

Questions?

