ESnet VPN Survey Dec 2011

*R. **Les Cottrell** & Guillaume Cessieux[SLAC],*

Presented at the ESCC meeting, Baton Rouge, Jan 2012

Why survey

- SLAC has just successfully completed a project to move users from Windows PPTP/VPN
- To Cisco AnyConnect (SSL/VPN)
  - Old system in place over a dozen years
  - New system driven by:
    - Improved coverage (more places allow it, Linux support, clientless/web access, improved reliability …)
    - Security

Experience

- Not as simple as previous system:
  - timeouts, no split tunneling, install client,
  - multiplicity of devices (Windows, Mac, Unix, iPhones, Androids, tablets, VMs), multiple OS release levels
  - Personal devices located in people homes
    - strange configurations and apps
    - home firewalls …
- Different, required user to do something, user inertia
- Moved over 855 users, lots of tracking & reminders
- Lots of training:
  - user support people, hand holding, reminders, email list
  - Documentation: how to, FAQs, trouble shoot etc

Survey overview

- Survey sent to ESCC email list 12/11/2011
- Responses were received by 4 days later
  - Thanks for quick responses
- Responses representing 13 Labs:
  - ANL, LANL, LBNL, JLAB, BNL, NREL, INL, FNAL, ESnet, GA, Ames, PPPL, SLAC
- ~ 73% (10) of responders were responsible for network support
- 7% (1) in user support
- 20% (3) other (All areas (2), IT chief engineer (1))

What Application do you use?

- 70% (9) of sites use Cisco VPN product (2 sites also use Cisco IPSec)
- 23% (3) use Juniper
- 7% (1) uses Checkpoint

Timeout – No activity

We do not have one	7.1%	1
<=15 mins	**28.6%**	**4**
<=30 mins	**28.6%**	**4**
<= 60 mins	21.4%	3
> 60 mins	14.3%	2

Timeout – re-authenticate

	%	Count
There is no re-authentication timeout	**50.0%**	**7**
<= 1 hour	7.1%	1
<= 4 hours	21.4%	3
<= 8 hours	7.1%	1
<= 12 hours	14.3%	2
<=25 hours	0.0%	0
> 25 hours	0.0%	0
	Other (please specify)	2

Timeout warning

- Eg. popup to allow reauthenticate so no disconnect
- 6 responses, 7 did not respond

	%	Count
No I do not know of this capability	33.3%	2
The application has such a capability built in and we use it (Checkpoint & Juniper)	**66.7%**	**4**
The application has such a capability, but we do NOT use it	0.0%	0
We implemented this feature ourself for our site	0.0%	0

Do you allow exceptions to timeouts

- Concern over managing
- 6 answers

	%	Count
No, we do not have such a process	**83.3%**	**5**
We don't have one now but we are studying whether to provide one	0.0%	0
We have a process but it is not used	16.7%	1
We have a process that grants an approved user no re-authentication timeout	0.0%	0
We have a process that grants an approved use an extended re-authentication timeout	0.0%	0

Other

- Based on survey convinced Security to extend re-authentication timeout from 8 to 12 hours
- SLAC final shutdown old Windows system no exceptions in December 2011
- Requested Cisco for a warning before re-authentication timeout
- See: confluence.slac.stanford.edu/display/NetMan/How+to+Connect+to+SLAC+VPN