Application and Virus Detecting Firewall on the SPring-8 Experimental User Network

Takashi SUGIMOTO, Miho ISHII, Toru OHATA,
Tatsuaki SAKAMOTO, and Ryotaro TANAKA
(JASRI/SPring-8)

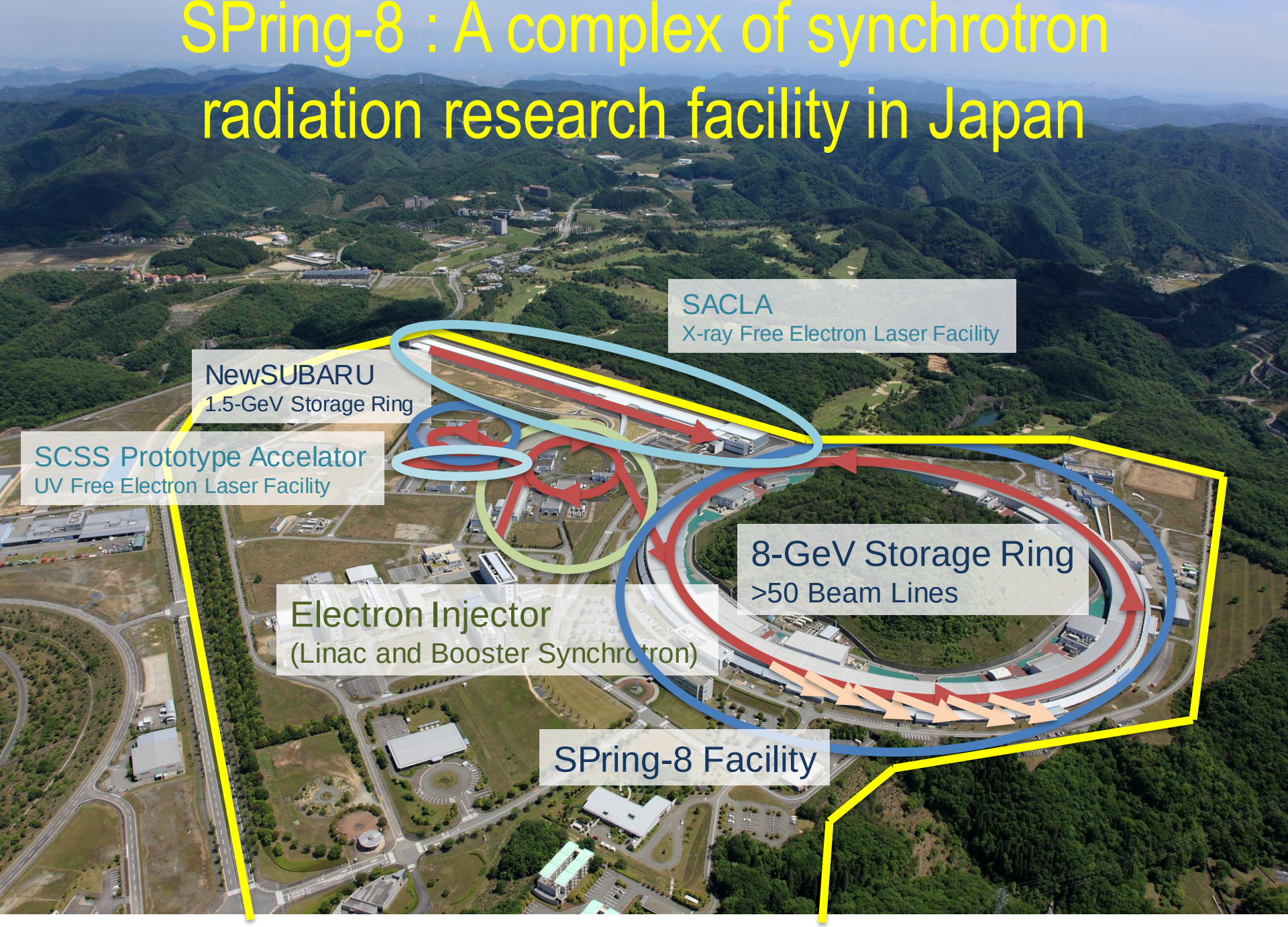
3rd Control System Cyber-Security Workshop,
WTC, Grenoble, France, October 9, 2011

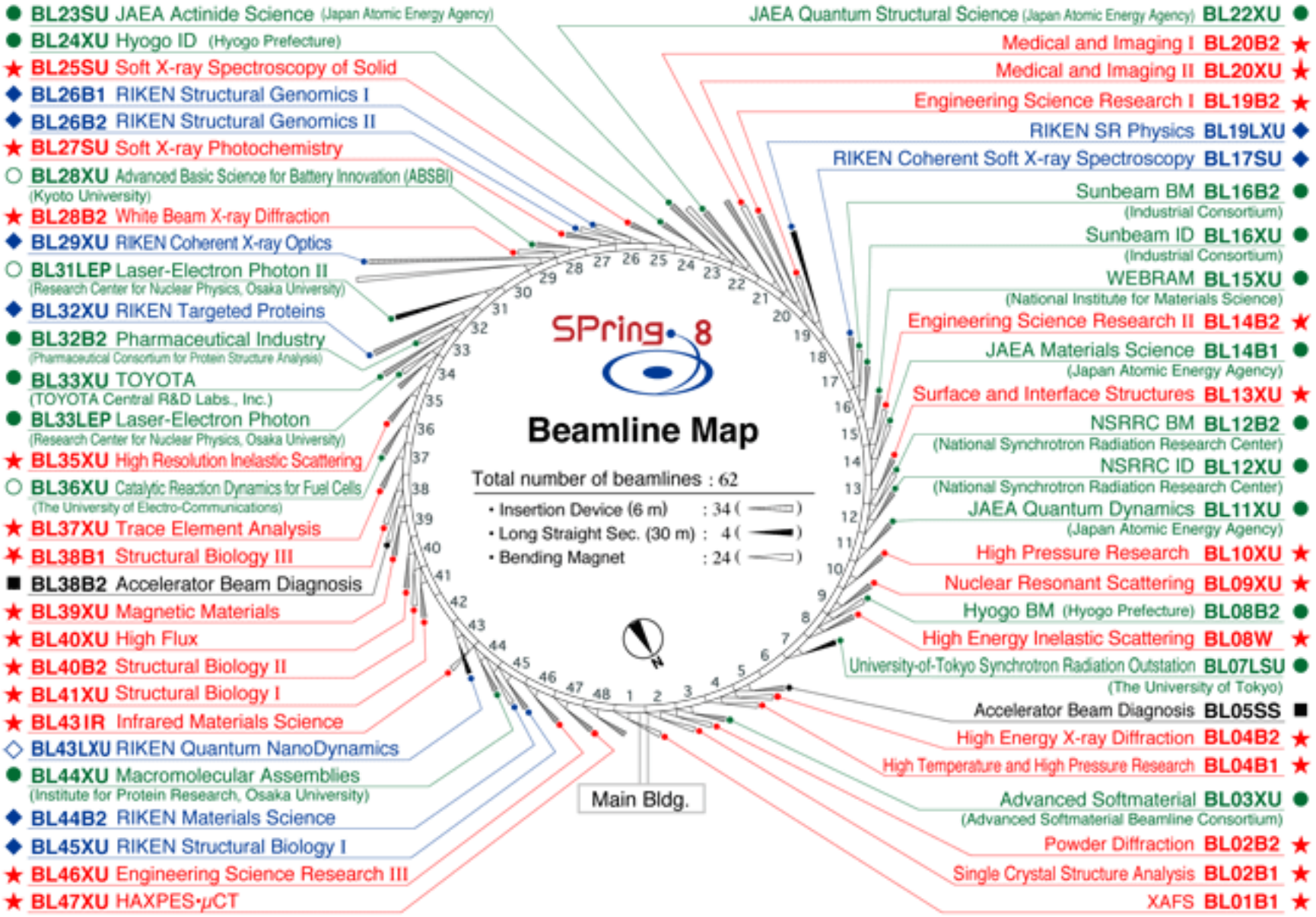
Contents

- Overview of SPring-8
- Problems on the Experimental User LAN
  - VPN, P2P, Virus
  - Solution: IPS (2004-)
- Recent Problems
  - Tunneling using HTTP(S)
- Replace the IPS by “Next Generation Firewall”
  - Evaluation and Install
- Summary

Overview of SPring-8

SPring-8 : A complex of synchrotron radiation research facility in Japan





We have 55 (operational) and 2 (under construction) beam lines (BLs).

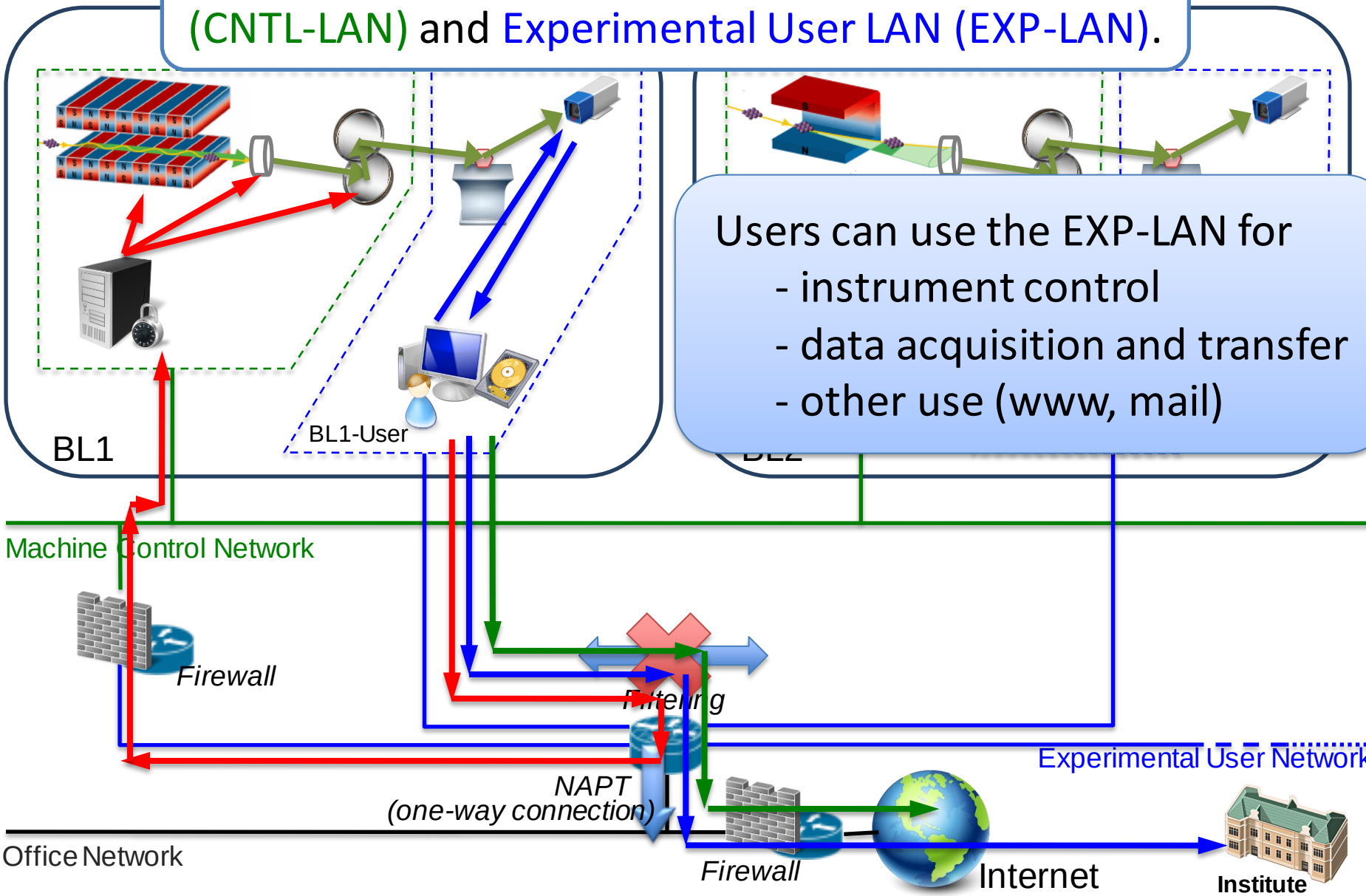
Experimental Users

- > 10,000 people visit the SPring-8 to perform experiments every year.
- Many people bring their own PCs
  - for experimental use (DAQ)
  - for their convenience (WWW, Mail, etc.)

- We prepare two ways to use their PCs.
  - Wi-Fi Access on Office-LAN
  - Experimental User LAN

Schematic View of Beamline Network

Each beamline has Machine Control Network (CNTL-LAN) and Experimental User LAN (EXP-LAN).



Problem on Experimental User LAN

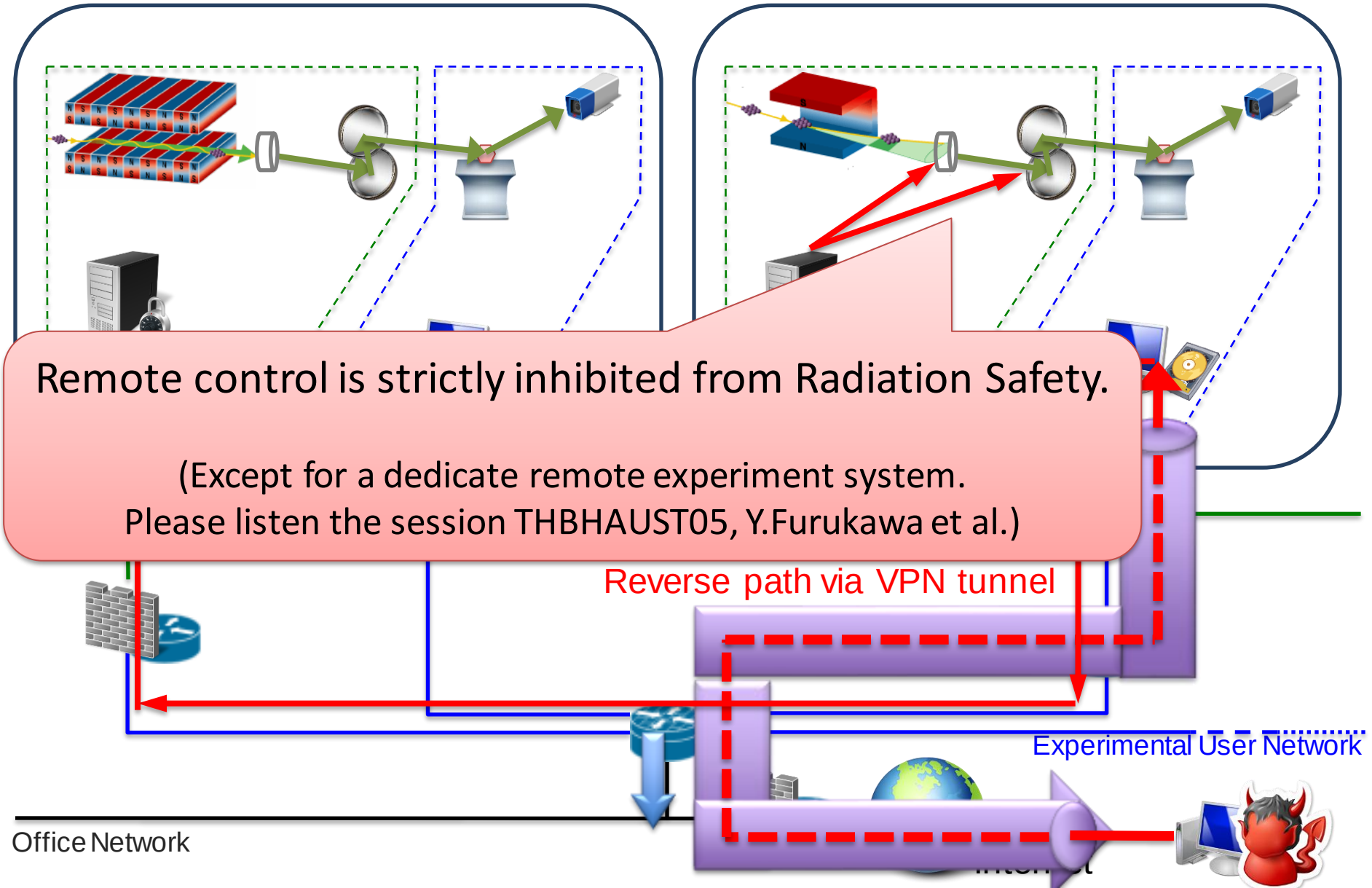
Problems on the EXP-LAN

- Unspecified number of people connect unmanaged PCs to the EXP-LAN
  - without any Authentication / Authorization / Accounting.

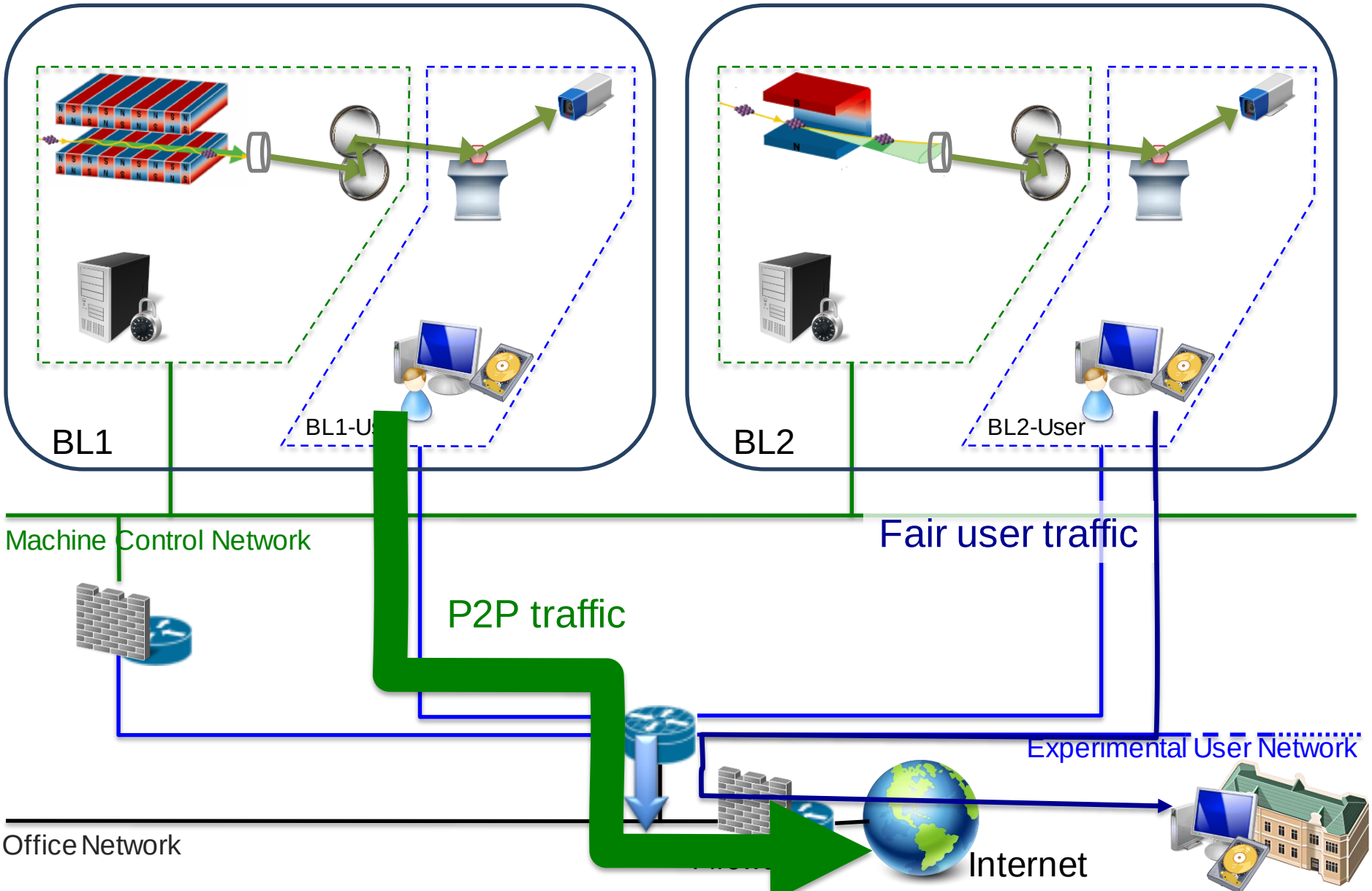
- Some people use unpermitted softwares
  - VPN
  - P2P file sharing
- Some PCs are infected by computer viruses.

Such applications threaten SPring-8 control system.

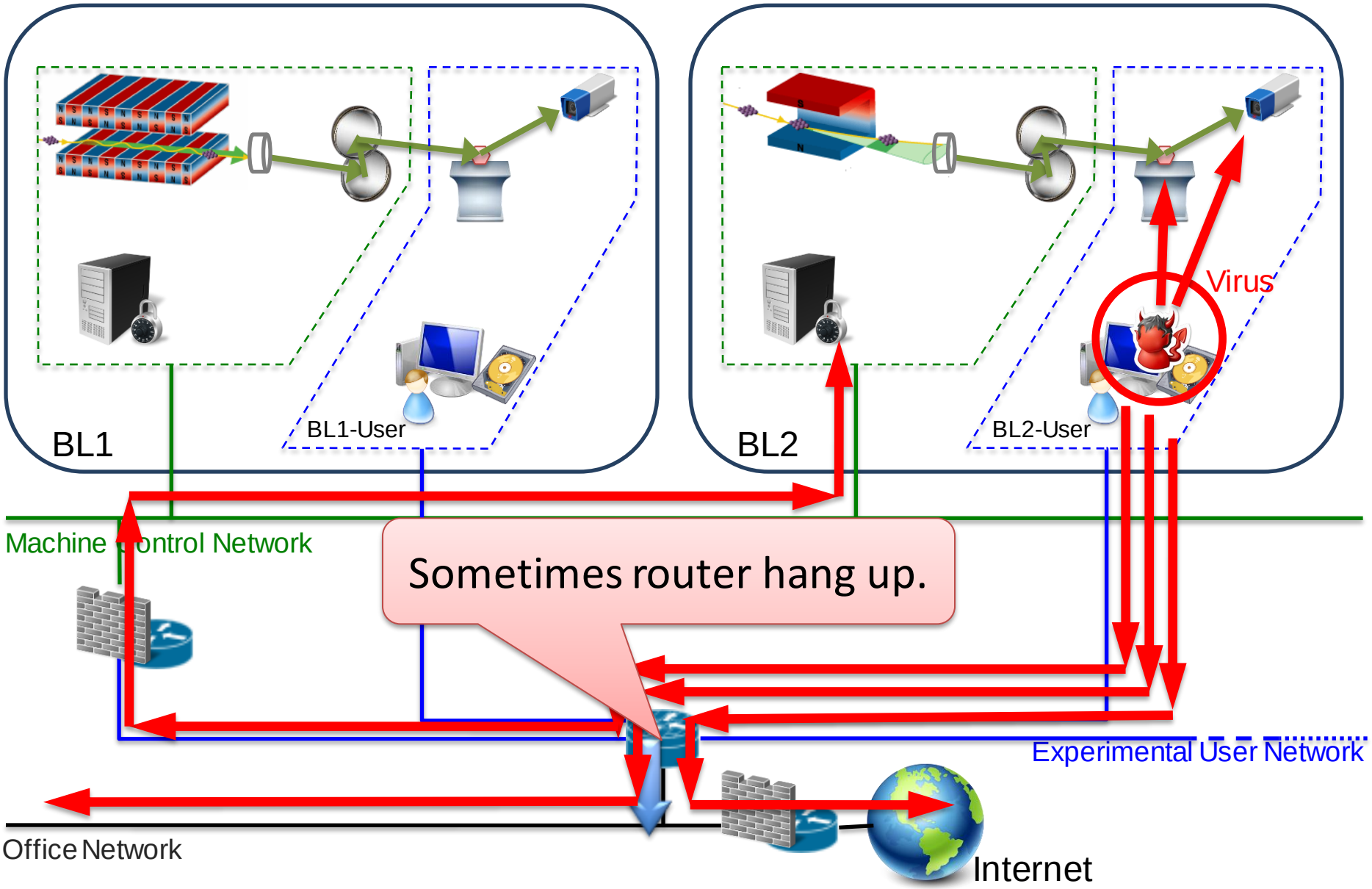
Problem1: Off-site Person can Control via VPN



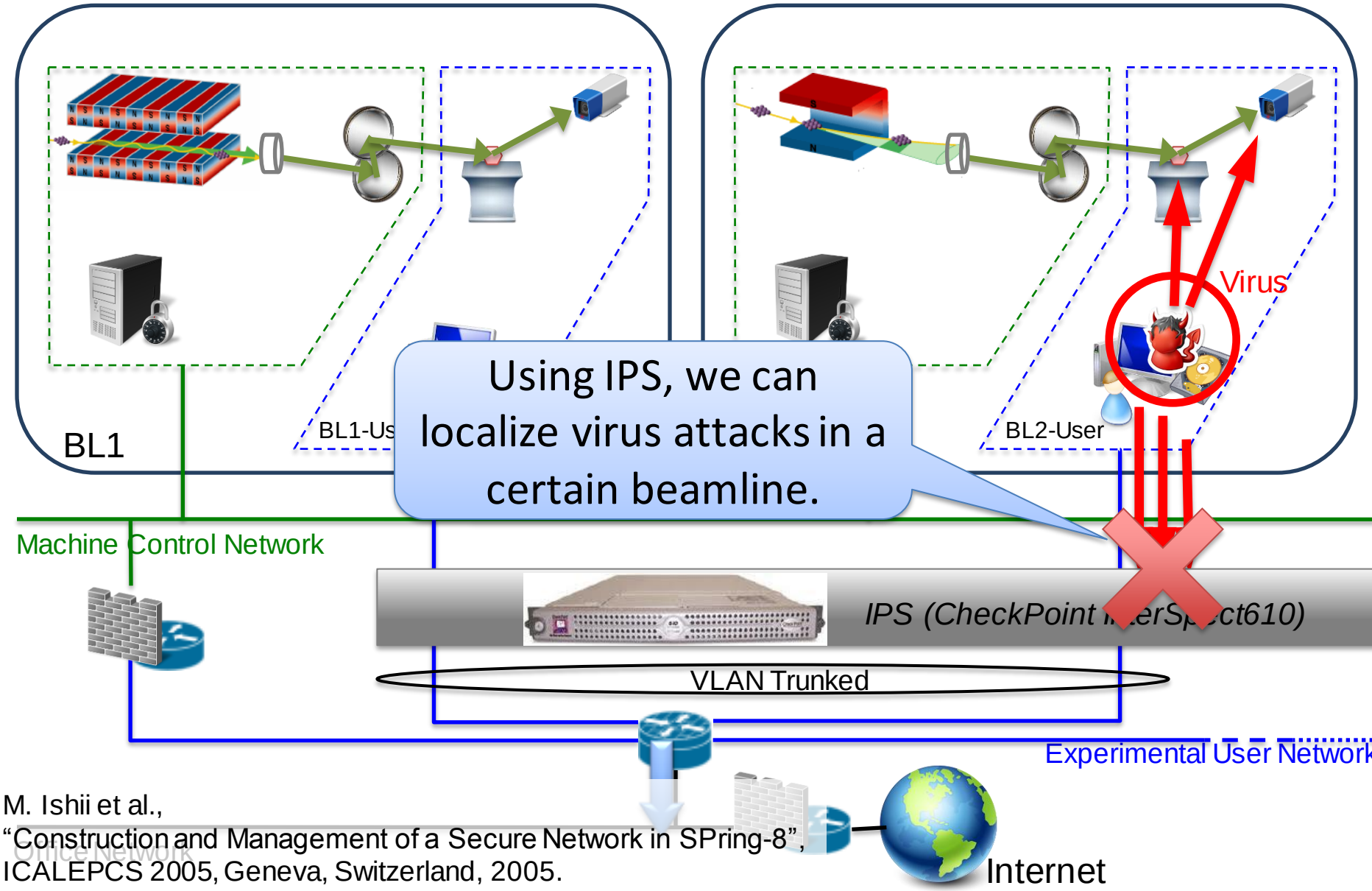
Problem2: Bandwidth Exhaution by P2P



Problem3: Virus Attack



Install Transparent IPS (2004-)

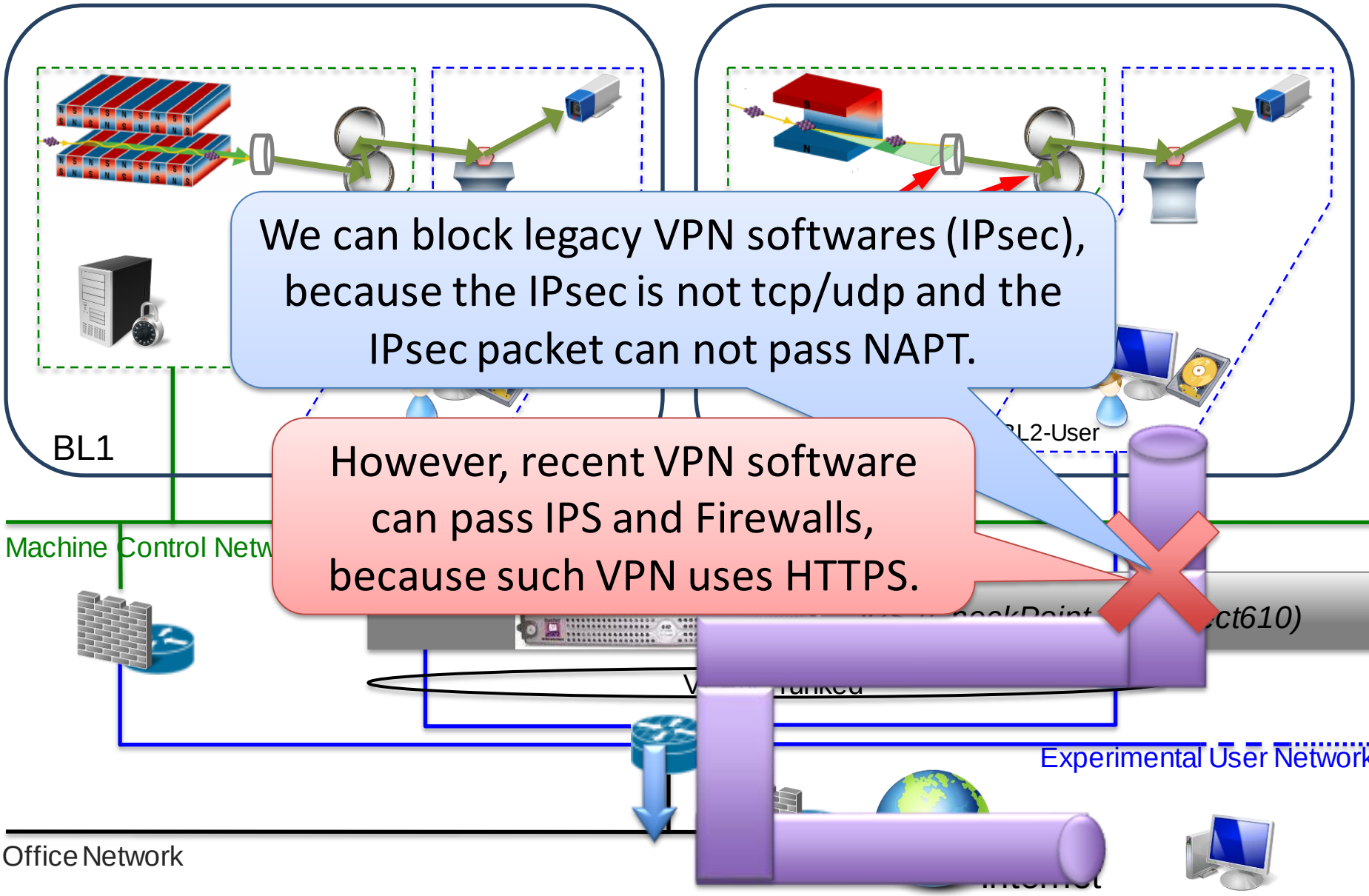


M. Ishii et al.,
"Construction and Management of a Secure Network in SPring-8",
ICALEPCS 2005, Geneva, Switzerland, 2005.

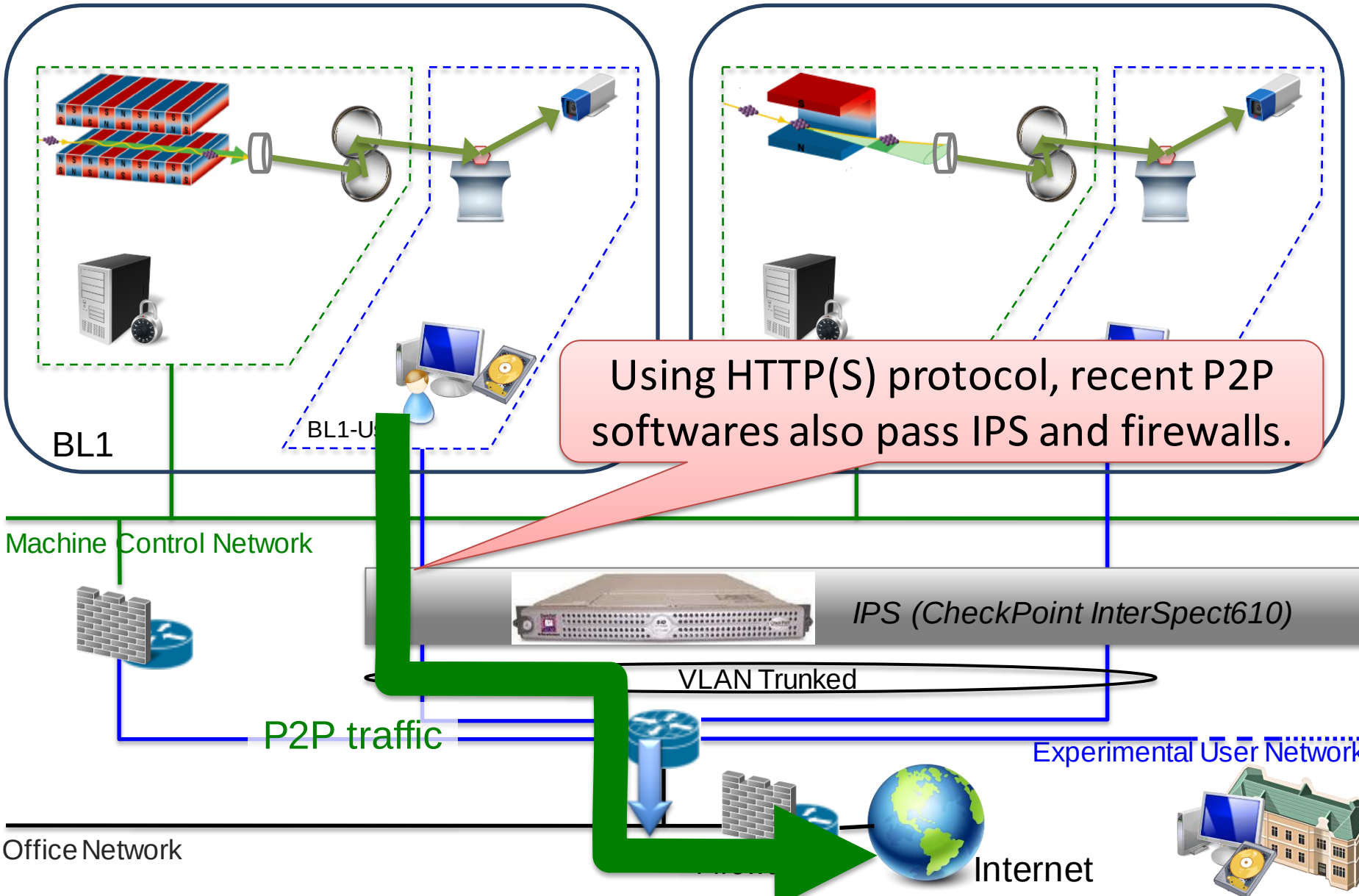
Recent Problem

Tunneling Applications

Problem1': Recent VPN Softwares



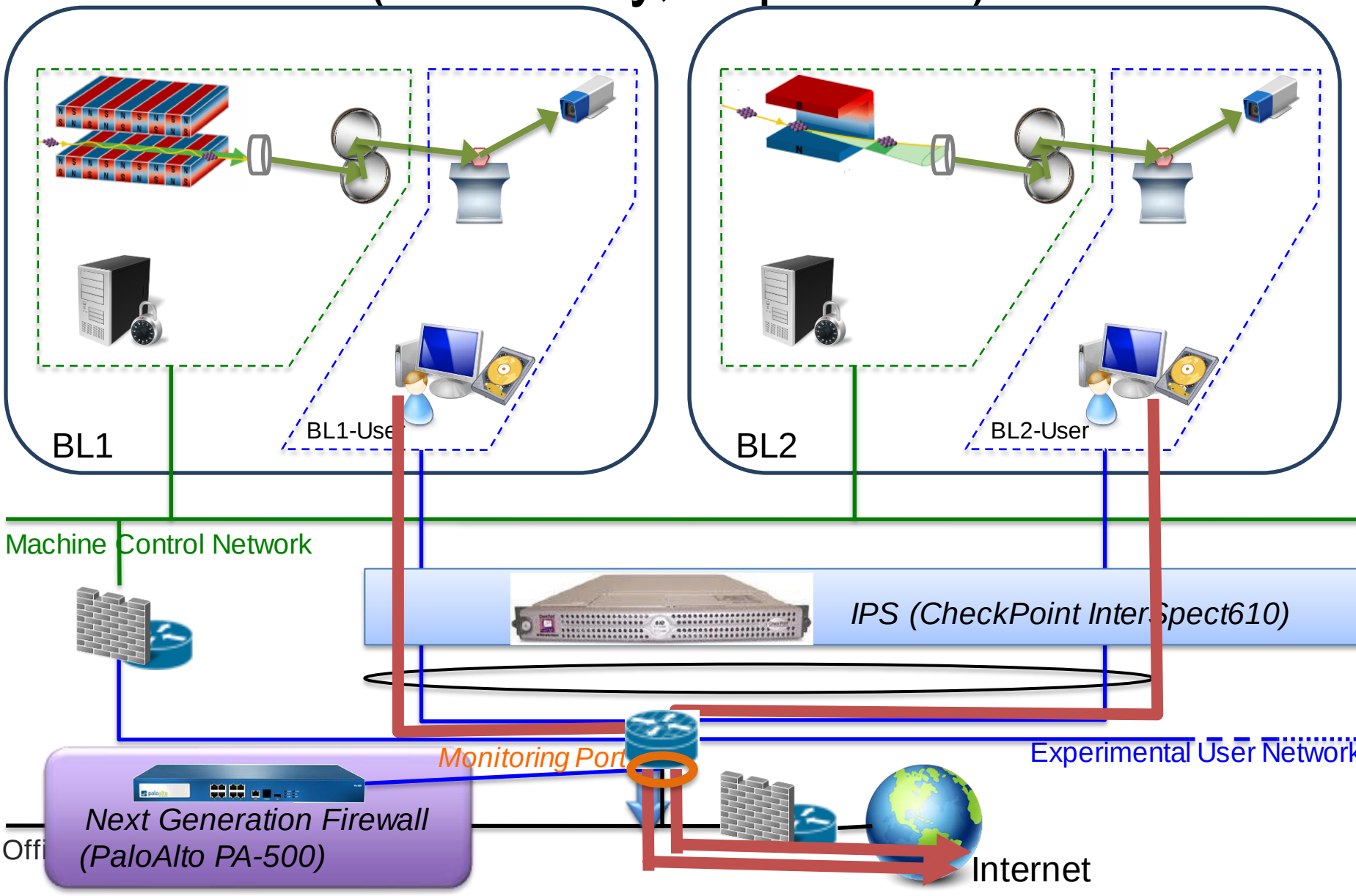
Problem2': Recent P2P Softwares



Replace IPS by “Next Generation Firewall”

Evaluation and Install

Evaluation of Next Generation Firewall (2010 July, Tap Mode)



Top 25 Applications (July 1 – 31, 2010)

Application Name	App Category	App Sub Category	Sessions	Bytes
ssh	networking	encrypted-tunnel	19950	1.27399E+12
ms-ds-smb	business-systems	storage-backup	11987	5.0741E+11
ftp	general-internet	file-sharing	3104107	3.80805E+11
nfs	business-systems	storage-backup	947	1.96318E+11
msrpc	networking	infrastructure	152	1.76369E+11
web-browsing	general-internet	internet-utility	3901184	1.46611E+11
unknown-tcp	unknown	unknown	224414	32607259839
afp	business-systems	storage-backup	82	19793808562
ssl	networking	encrypted-tunnel	823229	13462982181
vnc	networking	remote-access	77	13400994449
ms-rdp	networking	remote-access	268	12864823274
ms-update	business-systems	software-update	63495	12578977829
youtube-base	media	photo-video	4371	9912155433
t.120	networking	infrastructure	75	9314941655
flash	general-internet	internet-utility	22164	7096398144
symantec-av-update	business-systems	software-update	360664	6374641953
megaupload	general-internet	file-sharing	640	5693441130
http-video	media	photo-video	4037	4047977554
apple-update	business-systems	software-update	6939	3965761049
ciscovpn	networking	encrypted-tunnel	150	2517729101
yahoo-douga	media	photo-video	5668	2295136130
active-directory	business-systems	auth-service	2	2017950348
dns	networking	infrastructure	2922411	1916582840
itunes	media	audio-streaming	1555	1823506527

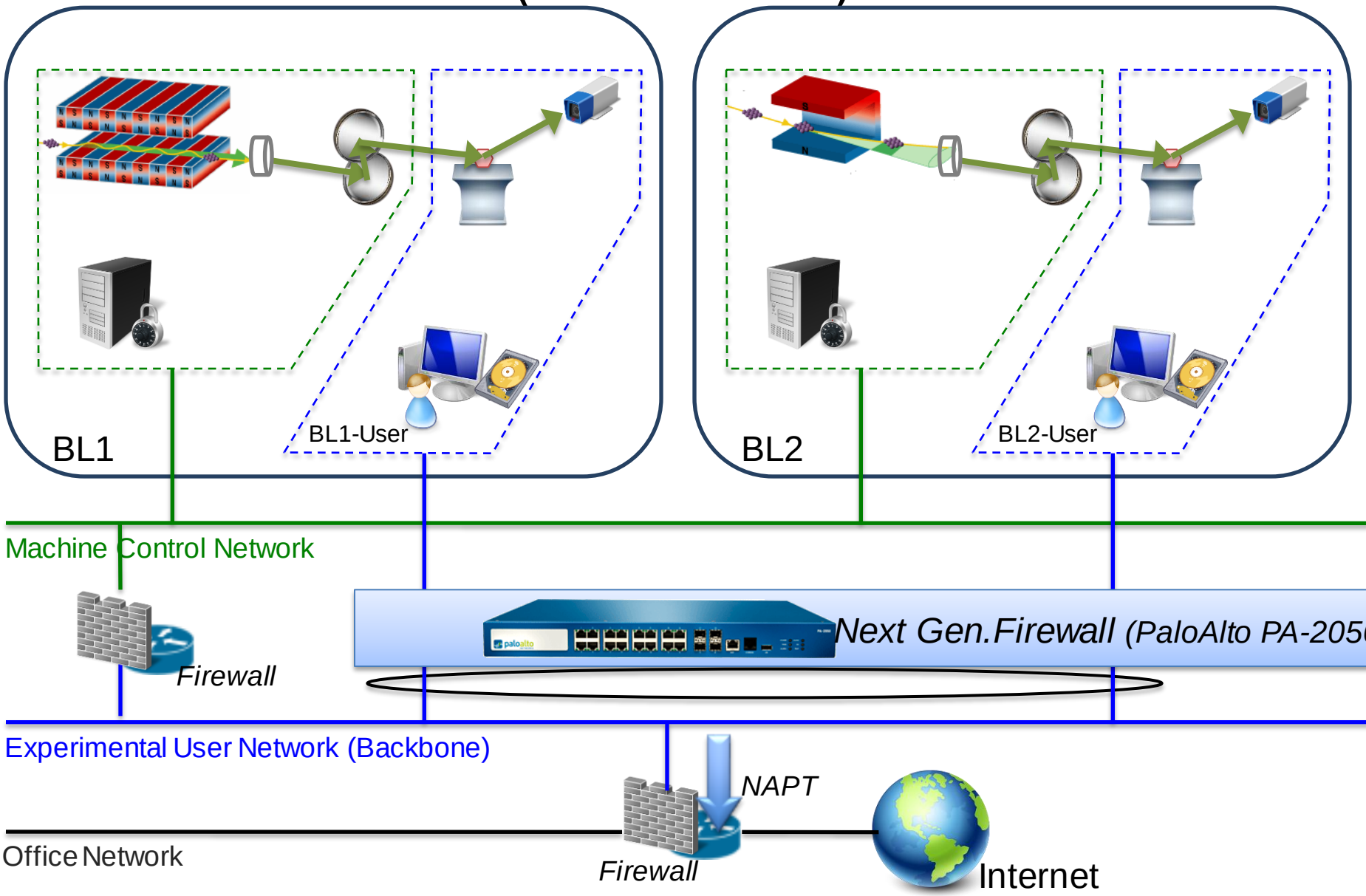
VPN (July 1 – 31, 2010)

Application Name	App Category	App Sub Category	Sessions	Bytes
ssh	networking	encrypted-tunnel	19950	1.27399E+12
ssl	networking	encrypted-tunnel	823229	13462982181
ciscovpn	networking	encrypted-tunnel	150	2517729101
ike	networking	encrypted-tunnel	12	114819257
ipsec-esp-udp	networking	encrypted-tunnel	22	57154472
tor	networking	encrypted-tunnel	19	5688367
open-vpn	networking	encrypted-tunnel	2	3602490

P2P File-sharing (July 1 – 31, 2010)

Application Name	App Category	App Sub Category	Sessions	Bytes
ftp	general-internet	file-sharing	3104107	3.80805E+11
megaupload	general-internet	file-sharing	640	5693441130
4shared	general-internet	file-sharing	91	364424179
webdav	general-internet	file-sharing	1232	293801170
msn-file-transfer	general-internet	file-sharing	130	13920462
rapidshare	general-internet	file-sharing	16	13142559
bittorrent	general-internet	file-sharing	31212	11921795
mediafire	general-internet	file-sharing	13	7734610
docstoc	general-internet	file-sharing	17	1437825
fs2you	general-internet	file-sharing	1108	1111203
office-live	general-internet	file-sharing	156	488310
akamai-client	general-internet	file-sharing	1903	390295
taku-file-bin	general-internet	file-sharing	41	335067
divshare	general-internet	file-sharing	2	295698
filestube	general-internet	file-sharing	12	190391
xunlei	general-internet	file-sharing	13	180090
nateon-file-transfer	general-internet	file-sharing	8	92186
emule	general-internet	file-sharing	864	91874
mydownloader	general-internet	file-sharing	1	76070
skydrive	general-internet	file-sharing	5	73139
flashget	general-internet	file-sharing	175	59396
qq-download	general-internet	file-sharing	49	30157
ares	general-internet	file-sharing	19	4186

Install the Next Generation Firewall (2010 Fall -)

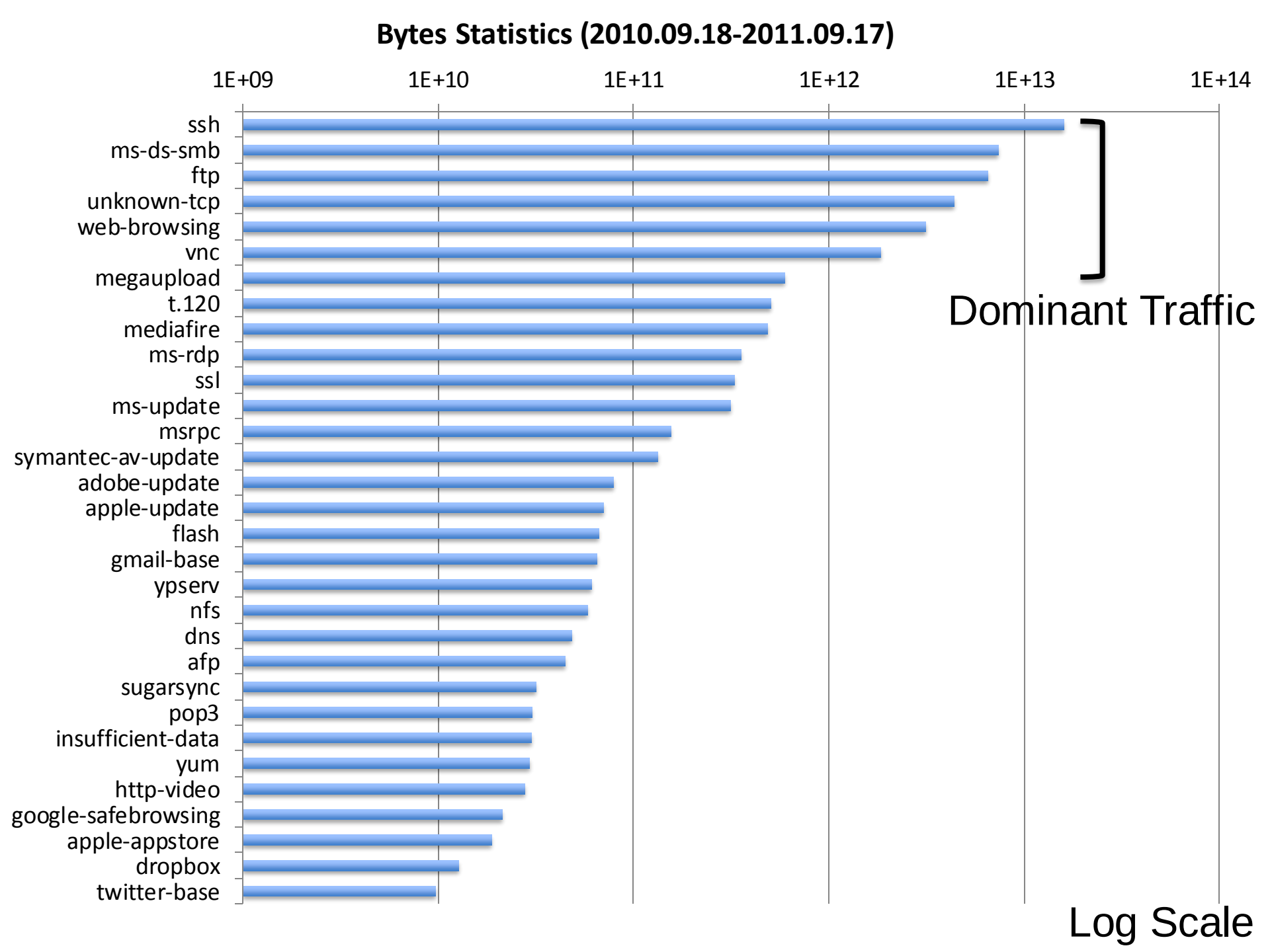


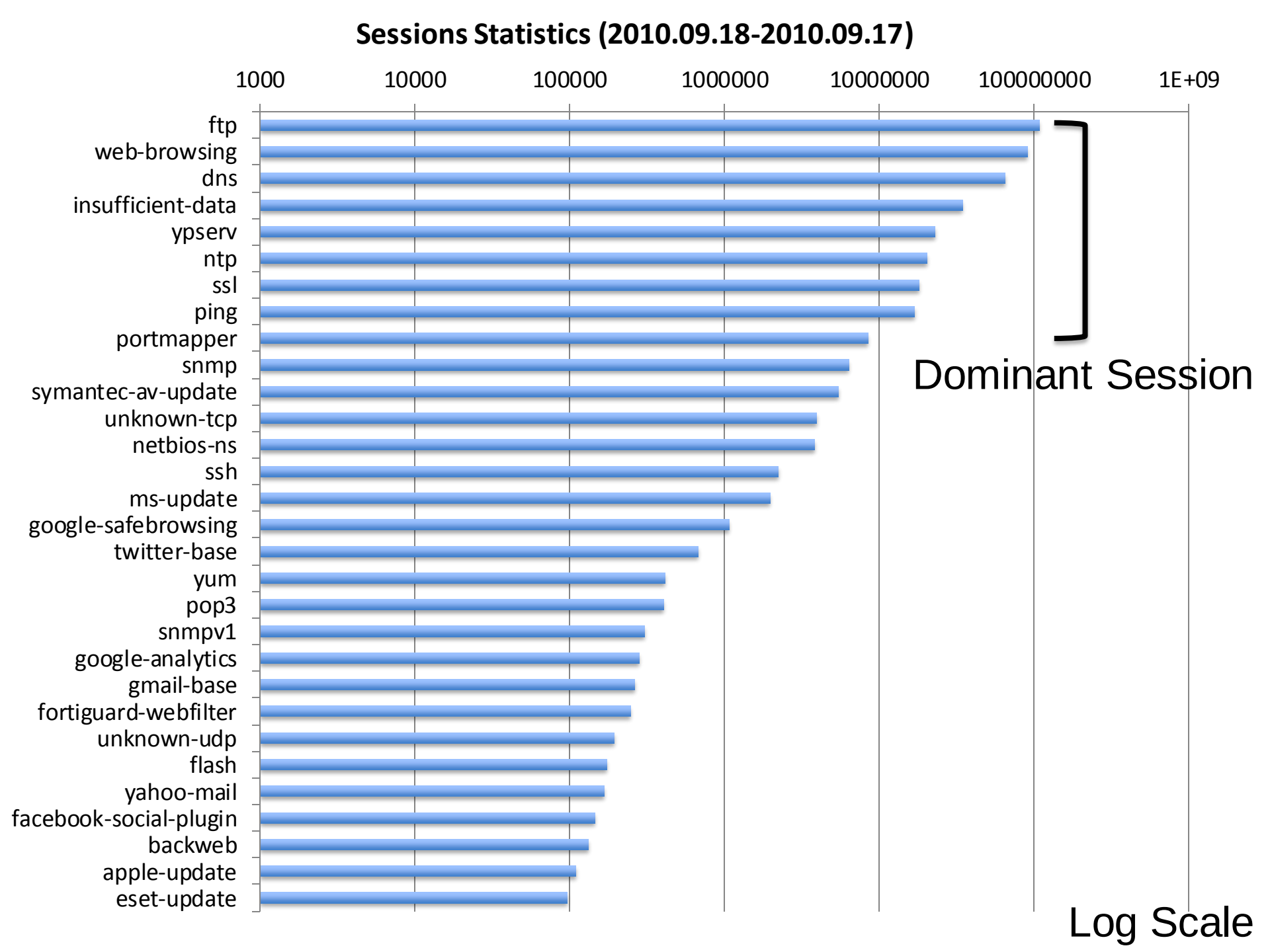
Top 25 Applications

(Sep. 18, 2010 – Sep. 17, 2011)

Application Name	App Category	App Sub Category	Sessions	Bytes
ssh	networking	encrypted-tunnel		
ms-ds-smb	business-systems	storage-backup		
ftp	general-internet	file-sharing		
unknown-tcp	unknown	unknown		
web-browsing	general-internet	internet-utility	91399894	3.14058E+12
vnc	unknown	unknown	537	1.84976E+12
megaupload	general-internet	file-sharing	25566	5.94995E+11
t.120	networking	infrastructure	3659	5.04735E+11
mediafire	general-internet	file-sharing	54593	4.867E+11
ms-rdp	networking	remote-access	5844	3.55244E+11
ssl	networking	encrypted-tunnel	18292920	3.28486E+11
ms-update	business-systems	software-update	1982952	3.14617E+11
msrpc	networking	infrastructure	587	1.55166E+11
symantec-av-update	business-systems	software-update	5511127	1.33698E+11
adobe-update	business-systems	software-update	50568	79289151276
apple-update	business-systems	software-update	110507	70339902358
flash	general-internet	internet-utility	174670	66448506565
gmail-base	collaboration	email	265601	65189109965
ypserv	networking	infrastructure	23206522	60955251082
nfs	business-systems	storage-backup	3351	58170163294
dns	networking	infrastructure	65959951	48338539879
afp	business-systems	storage-backup	7024	44794302217
sugarsync	general-internet	file-sharing	6223	31676171151
pop3	collaboration	email	405857	30227947749
insufficient-data	unknown	unknown	34785105	30103697318

We also found many people use on-line storage services.


Bytes Statistics (2010.09.18-2011.09.17)
1E+09
1E+10
1E+11
1E+12
1E+13
1E+14
ssh
ms-ds-smb
ftp
unknown-tcp
web-browsing
vnc
megaupload
t.120
mediafire
ms-rdp
ssl
ms-update
msrpc
symantec-av-update
adobe-update
apple-update
flash
gmail-base
ypserv
nfs
dns
afp
sugarsync
pop3
insufficient-data
yum
http-video
google-safebrowsing
apple-appstore
dropbox
twitter-base
Dominant Traffic
Log Scale


Sessions Statistics (2010.09.18-2010.09.17)
1000
10000
100000
1000000
10000000
100000000
1E+09
ftp
web-browsing
dns
insufficient-data
ypserv
ntp
ssl
ping
portmapper
snmp
symantec-av-update
unknown-tcp
netbios-ns
ssh
ms-update
google-safebrowsing
twitter-base
yum
pop3
snmpv1
google-analytics
gmail-base
fortiguard-webfilter
unknown-udp
flash
yahoo-mail
facebook-social-plugin
backweb
apple-update
eset-update
Dominant Session
Log Scale

Top 25 Threats (Viruses and Attacks)

(Sep. 18, 2010 – Sep. 17, 2011)

Threat Name	Application	App Category	App Sub Category	Count
Microsoft Windows SMB Fragmentation RPC Request Attempt	ms-ds-smb	business-systems	storage-backup	287642
FTP: login brute force attempt	ftp	general-internet	file-sharing	28031
Conficker DNS Request	dns	networking	infrastructure	18621
Trojan-Rustock.Phonehome	web-browsing	general-internet	internet-utility	13990
Rustock.Gen Command and Control Traffic	web-browsing	general-internet	internet-utility	13149
SMB: User Password Brute-force Attempt	ms-ds-smb	business-systems	storage-backup	4047
Trojan-Spy/Win32.spyeyes.nrn	java-update	business-systems	software-update	585
Microsoft Windows SMB Fragmentation RPC Request Attempt	ms-ds-smb	business-systems	storage-backup	339
WhenU_SaveNow Post installation download	web-browsing	general-internet	internet-utility	149
Geral User-Agent Traffic	web-browsing	general-internet	internet-utility	114
Microsoft Visual Basic VBP Project File Handling Buffer Overflow	ms-ds-smb	business-systems	storage-backup	102
Microsoft DCE RPC Big Endian Evasion Vulnerability	ms-ds-smb	business-systems	storage-backup	88
Microsoft DCE RPC Big Endian Evasion Vulnerability	msrpc	networking	infrastructure	87
Trojan/Win32.ruskill.eiq	ms-ds-smb	business-systems	storage-backup	75
MySQL MaxDB Webtool HTTP Request Parsing Buffer Overflow Vulnerability	web-browsing	general-internet	internet-utility	67
SMB: User Password Brute-force Attempt	ms-ds-smb	business-systems	storage-backup	58
TCP Flood	not-applicable	unknown	unknown	55
Trojan-Banker/Win32.banbra.tly	web-browsing	general-internet	internet-utility	53
ClamAV libclamav PE File Handling Integer Overflow Vulnerability	ms-ds-smb	business-systems	storage-backup	49
WhenU_SaveNow Ads data retrieve	web-browsing	general-internet	internet-utility	46
Trojan/Win32.ruskill.eiq	ms-ds-smb	business-systems	storage-backup	44
Microsoft Visual Basic VBP Project File Handling Buffer Overflow	ms-ds-smb	business-systems	storage-backup	42
HTTP Cross Site Scripting Attempt	web-browsing	general-internet	internet-utility	40
FTP evasion attack	ftp	general-internet	file-sharing	34
Microsoft Windows RPC Encrypted Data Detected	ms-ds-smb	business-systems	storage-backup	33

Performance of the Next Gen. Firewall

(Sep. 18, 2010 – Sep. 17, 2011)

PaloAlto PA-2050

- Detect and Filter Applications
  - 287 applications are detected.
  - No VPN nor P2P applications passed through.
- Detect and Filter Viruses and those Attacks
  - 140 viruses/attacks are detected and filtered.
  - Virus signature is updated every day.

- Another Merit
  - We can plan next service by utilizing the application statistics. (e.g. Large-bandwidth, large-capacity on-line strorage service)

The updated EXP-LAN with next generation firewall works good for one year without fatal trouble. ☺

Summary

- We replaced IPS by “Next Generation Firewall”.
- “Next Generation Firewall” works good.
  - The next generation firewall detects and blocks many inhibited applications.
    - VPN software, which break radiation security
    - P2P software, which cause bandwidth exhaustion
    - Computer Viruses
  - We also utilize application statistics for planning next service.
    - On-line storage service for experimental users.