NETFORT
know your network

Five Key Challenges Facing Campus Network Administrators Today

Real-world solutions for improving the security and productivity of students, educators and administrators

Introduction:

Shouldering the Responsibilities of a Campus Network

Networking and IT Professionals today have a tremendous responsibility when it comes to managing the network of a higher-education campus or organization. The massive growth of stored data (and the need to share it) is constantly placing pressure on an already over-stressed network. The unpredictable student user base is prone to network misuse and security breaches. Educators are looking to further leverage networked-based learning tools and streaming video. Campus administrators are adding new applications while demanding more and more remote accessibility; and campus legal departments are anxious to ensure that campus networks are meeting all government and other security and privacy regulations and compliancy—while constantly making requests for network usage reports and other network activity to assist in copyright protection efforts.

The Campus Networking Environment

Networking and IT Professionals responsible for the management of an organizational-wide network within a higher-education institution such as a college, university or other learning institutes are faced with one of the most challenging networking environments today. The parameters that exist for campus networking environments are numerous and daunting:

- Large network extended across broad geographies
- Massive user base that is constantly in a state of change
- Complex networking infrastructures across diverse platforms
- Strong need to track individual user activity due to copyright infringement concerns, cheating, etc.
- Wide array of network devices of all types, makes, operating systems, etc.
- High number of remote and transient users
- Broad and disparate number of applications and databases being accessed across the network
- Unpredictable user base (especially students) apt to misuse or attempt to breach network security
- High volume of large file sharing and file downloading
- Open networks (required especially for remote access) creating higher security risk

The fact is clear: there is unlikely a networking environment today as challenging and as complex as exists at colleges, universities and higher-education institutes.

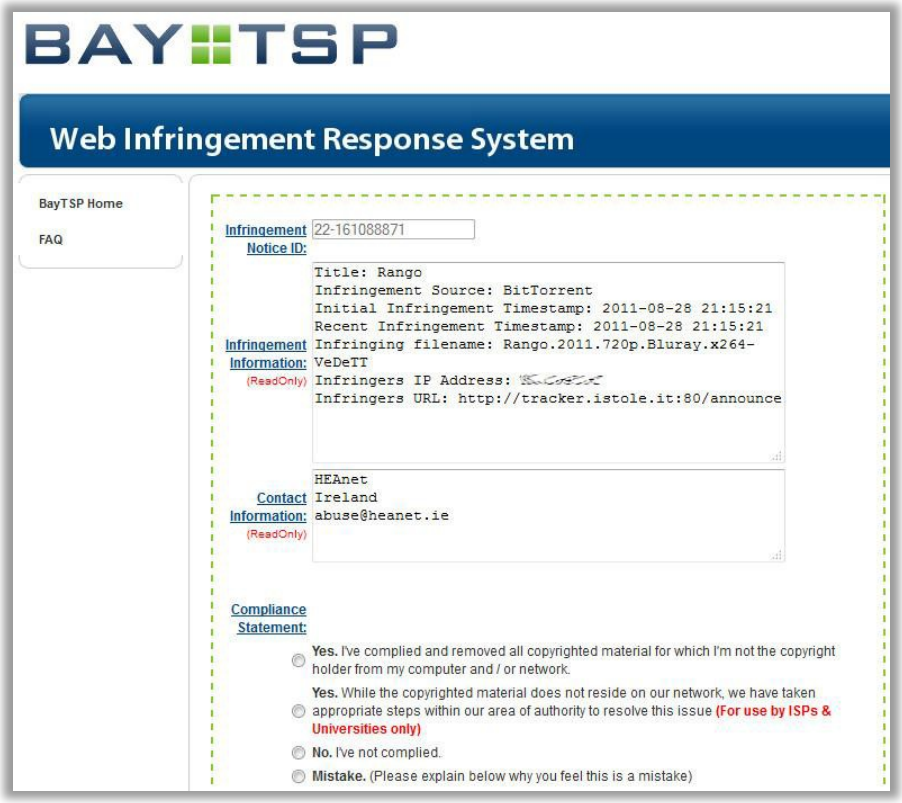
The NetFort LANGuardian Campus Network Challenges | White Paper

This white paper sets out to discuss five specific and key challenges that are faced by campus network professionals today – and provide real-world examples of how colleges, universities and higher education learning institutions have been able to address these key challenges with the use of NetFort LANGuardian™, a powerful software tool that helps monitor and manage the traffic flow across campus networks, recording and tracking details of user activity and traffic volumes, while generating reports on the health and security of the network.

It also discusses these five actual scenarios, where campus networking professionals were faced with some of the most common, yet critical challenges in managing, monitoring and securing their campus network—to improve the security and productivity of students, educators and administrators.

Campus Network Challenge #1: Responding to copyright infringement requests

Colleges and universities have an obligation to promptly investigate issues brought to their attention by an external source. These may vary from notifications about network scanning to inquiries regarding downloaded files. The following is an actual example of where HEAnet – (Ireland's National Education and Research Network, which provides high quality Internet services to Irish universities, institutes, and the education and research communities) has been notified of copyrighted material being downloaded onto a campus network via BitTorrent:



The Answer

A review of the main LANGuardian security report revealed a number of users running BitTorrent at the time referenced in the notification. LANGuardian's intrusion detection records and historical database were used to identify the issue. What proved of particularly high value to the campus network team was the fact that the LANGuardian system can link back to the individual username. Tracking network activity to individual username levels allows much more specific and timely response to important third party inquiries regarding questionable or concerning network activity.

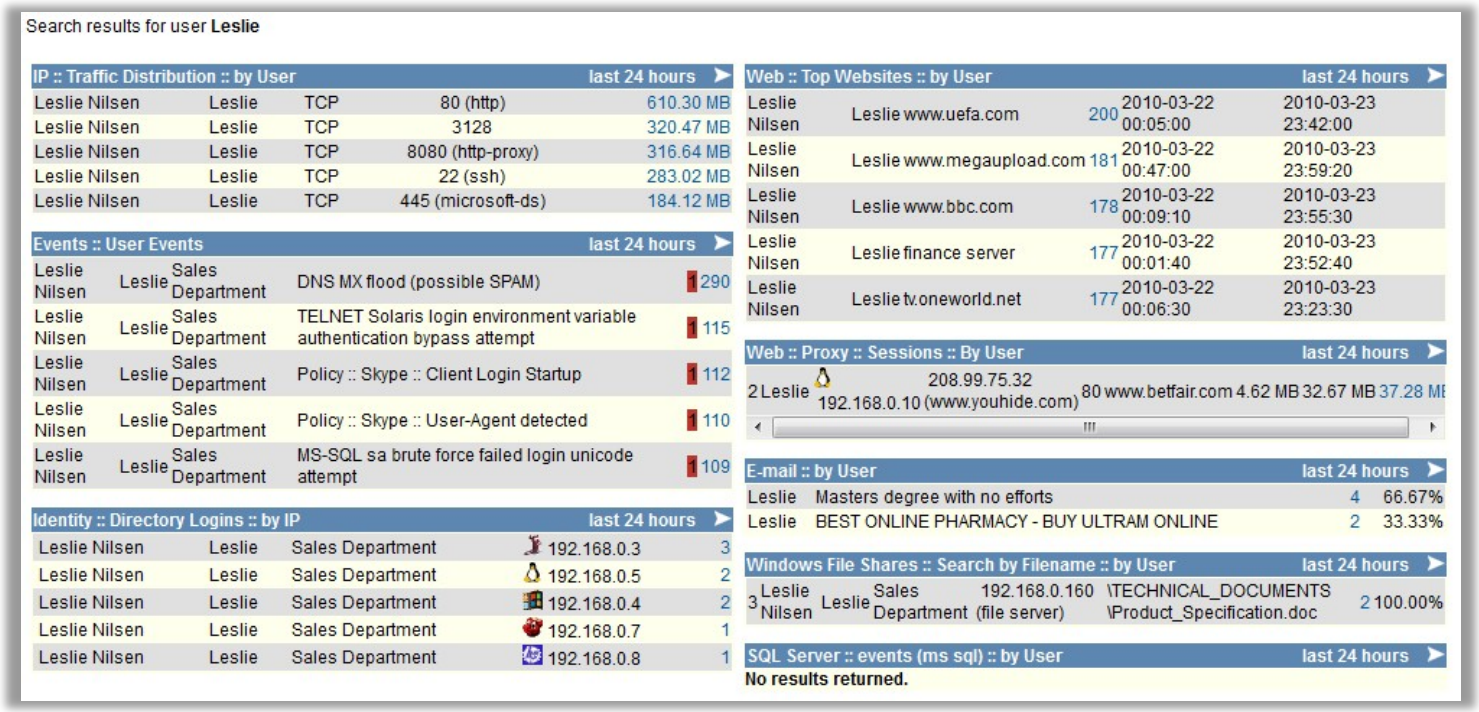
Full Name	Logon Name	TRACKER	INFO_HASH	TORRENT	Source	Destination	Time
Fred Dandy	Fred	tracker.publicbt.com	52e6eb94135329ad2852079dfcdde69021176785	Not Found	192.168.0.4	85.17.80.248 (tracker.publicbt.com)	2010-03-23 16:01:40
Peter Erwin	Peter	torrent.ubuntu.com:6969	c4ed23adb9bd34bc35a815f903ab24ff20d9163c	Not Found	192.168.0.5	91.189.90.143	2010-03-23 16:01:40

Go to: 1 Show rows: 10 1 of 1

Campus Network Challenge #2: Investigating the network activity of an individual student or staff member

There are many reasons why network administrators and managers need to have the ability to focus on a specific student or staff member. Recently, a customer used LANGuardian's user search feature to focus attention and investigation on a member of staff who had clicked on a link within an email, causing their PC to become infected with malware—which, in turn, started to send massive quantities of SPAM email.

The network administrators wanted to check what other systems were accessed by the problematic PC. It was easily done using the LANGuardian user search feature. The image below shows a similar report that was generated by LANGuardian.



Search results for user **Leslie**

IP :: Traffic Distribution :: by User — last 24 hours

Leslie Nilsen	Leslie	TCP	80 (http)	610.30 MB
Leslie Nilsen	Leslie	TCP	3128	320.47 MB
Leslie Nilsen	Leslie	TCP	8080 (http-proxy)	316.64 MB
Leslie Nilsen	Leslie	TCP	22 (ssh)	283.02 MB
Leslie Nilsen	Leslie	TCP	445 (microsoft-ds)	184.12 MB

Events :: User Events — last 24 hours

Leslie Nilsen	Leslie	Sales Department	DNS MX flood (possible SPAM)	1 290
Leslie Nilsen	Leslie	Sales Department	TELNET Solaris login environment variable authentication bypass attempt	1 115
Leslie Nilsen	Leslie	Sales Department	Policy :: Skype :: Client Login Startup	1 112
Leslie Nilsen	Leslie	Sales Department	Policy :: Skype :: User-Agent detected	1 110
Leslie Nilsen	Leslie	Sales Department	MS-SQL sa brute force failed login unicode attempt	1 109

Identity :: Directory Logins :: by IP — last 24 hours

Leslie Nilsen	Leslie	Sales Department	192.168.0.3	3
Leslie Nilsen	Leslie	Sales Department	192.168.0.5	2
Leslie Nilsen	Leslie	Sales Department	192.168.0.4	2
Leslie Nilsen	Leslie	Sales Department	192.168.0.7	1
Leslie Nilsen	Leslie	Sales Department	192.168.0.8	1

Web :: Top Websites :: by User — last 24 hours

Leslie Nilsen	Leslie www.uefa.com	200	2010-03-22 00:05:00	2010-03-23 23:42:00
Leslie Nilsen	Leslie www.megaupload.com	181	2010-03-22 00:47:00	2010-03-23 23:59:20
Leslie Nilsen	Leslie www.bbc.com	178	2010-03-22 00:09:10	2010-03-23 23:55:30
Leslie Nilsen	Leslie finance server	177	2010-03-22 00:01:40	2010-03-23 23:52:40
Leslie Nilsen	Leslie tv.oneworld.net	177	2010-03-22 00:06:30	2010-03-23 23:23:30

Web :: Proxy :: Sessions :: By User — last 24 hours

2	Leslie	208.99.75.32 192.168.0.10 (www.youhide.com)	80	www.betfair.com	4.62 MB	32.67 MB	37.28 MB

E-mail :: by User — last 24 hours

Leslie	Masters degree with no efforts	4	66.67%
Leslie	BEST ONLINE PHARMACY - BUY ULTRAM ONLINE	2	33.33%

Windows File Shares :: Search by Filename :: by User — last 24 hours

3	Leslie Nilsen	Leslie	Sales Department	192.168.0.160 (file server)	\TECHNICAL_DOCUMENTS \Product_Specification.doc	2	100.00%

SQL Server :: events (ms sql) :: by User — last 24 hours

No results returned.

In this case, LANGuardian's network traffic analysis deep packet inspection, Active Directory user information and historical database were leveraged to drill down into the individual user's detailed network activity (by username) to identify the problem and source of the malware.

Campus Network Challenge #3: Watching out for DDoS activity

A recent article from the BBC suggests that website-crippling cyber-attacks are to rise in 2016. The majority of these were NTP amplification attacks. NTP is a vector for DDoS attacks because, like DNS, it is a simple UDP-based protocol that can be persuaded to return large replies to small requests. How can we check if our network is under attack?

The Answer

When it comes to mitigating against DDoS attacks, you have a number of options. It depends on what stage you are at. If you are presently under attack, you may need to weather the storm a little and avoid any rash decisions. Blocking traffic for example may only introduce other problems and you may end up with a network cut off from the outside world.

It is critical that you have some type of network activity monitoring in place prior to and during an attack. Make sure you can see where the traffic is coming from and what servers are being targeted. To mitigate against an attack, you should consider the following.

1. Check if your ISP can black hole the suspicious traffic. Most will not get involved, but if you are an education or a government institute you may be able to address the issue at an ISP level.
2. If you host your own web applications or servers you could consider a local DDoS protection system. These high-performance appliances enable attack traffic analysis and cleaning of the traffic, enabling a defense against large-scale DDoS attacks. Good traffic goes one way and bad traffic is dropped.
3. If your website is hosted externally, you could consider something like the Cloudflare DDoS protection infrastructure. They do the job of sorting out the good traffic from the bad in the cloud.
4. In some extreme cases, companies have changed their ISP to get away from the problem. Their public IP addresses appear to be a constant target, so the only way out is to change them is by moving to a different ISP.

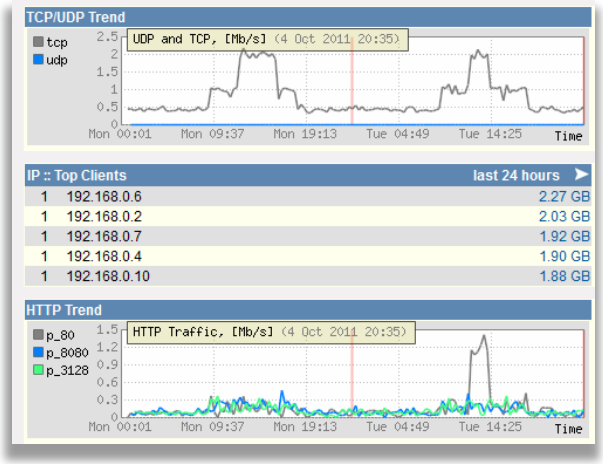
Campus Network Challenge #4:
Determining why applications are slowing down

On 24th December, 2014 one of Ireland's prestigious universities contacted the NetFort support team requesting assistance to help with a problem, where their Blackboard application was going off-line. This was a massive problem as staff and students needed to access this application over the Christmas holiday period. At first, they suspected a DDoS attack, but were unsure. With this critical application going off-line, the entire academic program was at risk of becoming completely unavailable to students and educators alike. So, the pressure mounted on the IT staff to find the problem and fix it fast.

The Answer

Using LANGuardian's network traffic analysis deep packet inspection capabilities, an analysis of the network traffic between the Blackboard servers showed large amounts of logon originating from Android based devices. Each device would logon but once authenticated, would continue to issue logon requests—eventually the logon process failed, causing the main application to be inaccessible. As a short-term measure, the network administrators blocked Android devices at the firewall and waited until the application was patched before they were allowed to connect again.

The screengrabs below show an example of a LANGuardian report that is focused on traffic levels and top clients on the network. Unusual activity can be quickly spotted for immediate action. By simply clicking on the trend peaks, you can drill down to get further information as needed—right down to the individual username level.



Sensor	Protocol	Service	Total Yesterday	Total Today	Percent yesterday	Percent today
11	TCP	443 (https)	82.41 MB	249.06 MB (+202%)	30.71	44.11
11	TCP	22 (ssh)	78.38 MB	57.36 MB (-26%)	29.20	10.16
11	UDP	161 (snmp)	37.20 MB	19.62 MB (-47%)	13.86	3.48
11	TCP	80 (http)	29.99 MB	178.74 MB (+495%)	11.17	31.66
11	TCP	993 (imap-secure)	16.99 MB	20.76 MB (+22%)	6.33	3.68
11	UDP	137 (netbios-ns)	2.65 MB	2.63 MB	0.99	0.47
11	UDP	1900 (upnp)	2.32 MB	2.03 MB (-12%)	0.87	0.36
11	UDP	17500	2.26 MB	1.32 MB (-41%)	0.84	0.23
11	TCP	445 (microsoft-ds)	1.52 MB	789.59 KB (-49%)	0.57	0.14
11	ICMP	(n/a)	885.91 KB	987.97 KB (+11%)	0.32	0.17

Similarly, NetFort worked with another college recently which was experiencing problems with a remote connection to a training center. Users at the site were complaining that accessing their systems was slow. Using LANGuardian, they found that user PCs at the center were automatically connecting back to a Windows update server and were downloading updates which resulted in large volumes of traffic. Because the PCs were not powered up regularly, they all downloaded updates at the same time. The update process was simply paused, allowing users to get on with work without experiencing delays with application responses. Identifying what was causing this problem would normally have been a difficult, time-consuming task; with LANGuardian, it took just minutes to detect the problem.

Campus Network Challenge #5:
Detecting Ransomware on the network

According to a new report from McAfee Labs, Ransomware continues to remain a major and rapidly growing threat in 2016. New variants of Ransomware are appearing on a daily basis and traditional security tools like antivirus are struggling to keep up. New variants have also changed the way they encrypt files and what happens your data once it is encrypted.

The Answer

5 tips for Detecting and alerting on the presence of Ransomware

1. Watch out for known file extensions

Even though the list of known Ransomware file extensions is growing rapidly, it is still a useful method for detecting suspicious activity. Before you do anything you need to get file activity monitoring in place so that you have both a real time and historical record of all file and folder activity on your network file shares.

There is an interesting discussion on this Reddit post which has a link to a number of resources including this spreadsheet which has a comprehensive list of all known Ransomware variants. We currently work off this list and you can use this on your LANGuardian to create a custom report. As the list is in Regex format, you may be able to use it on other monitoring systems.

\.enc|\.R5A|\.R4A|\.encrypt|\.locky|\.clf|\.lock|\.cerber|\.crypt|\.txt|\.coverton|\.enigma|\.czvxce|\.{CRYPTENDBLACKDC}|\.scl|\.crinf|\.crjoker|\.encrypted|\.code|\.CryptoTorLocker2015!|\.crypt|\.ctbl|\.html|\.locked|
\.ha3|\.enigma|\.html|\.cry|\.crime|\.btc|\.kkk|\.fun|\.gws|\.keybtc@inbox_com|
\.kimcilware.LeChiffre|\.crime|\.oor|\.magic|\.fucked|\.KEYZ|\.KEYH0LES|\.crypted|\.LOL!|\.OMG!|\.EXE|\.porno|\.RDM|\.RRK|
\.RADAMANT|\.kraken|\.darkness|\.nochance|\.oshit|\.oplata@qq_com|\.relock@qq_com|\.crypto|\.helpdecrypt@ukr|\.net|\.pizda@qq_com| \.dyatel@qq_com_ryp|\.nalog@qq_com|
\.chifrator@qq_com|\.gruzin@qq_com|\.troyancoder@qq_com|\.encrypted|\.cry|
\.AES256|\.enc|\.hb15|\.vscrypt|\.infected|\.bloc|\.korrektor|\.remind|\.rokku|\.encryptedAES|\.encryptedRSA|
\.encedRSA|\.justbtcwillhelpyou|\.btcbtcbtc|\.btc-help-you| \.only-we_can-help_you|\.sanction|\.sport|\.surprise|\.vvv|\.ecc|\.exx|\.ezz|\.abc|\.aaa|\.zzz|\.xyz|\.biz|\.micro|\.xxx|\.ttt|\.mp3|\.Encrypted|
\.better_call_saul|\.xtbl|\.enc|\.vault|\.xort|\.trun|\.CrySiS|\.EnCiPhErEd|\.73i87A|\.p5tkjw|\.PoAr2w|\.xrtn|\.vault|\.PORNO

2. Watch out for an increase in file renames

File renames are not a common action when it comes to activity on network file shares. Over the course of a normal day, you may end up with just a handful of renames even if you have hundreds of users on your network. When Ransomware strikes, it will result in a massive increase in file renames as your data gets encrypted.

You can use this behavior to trigger an alert. However, if the number of renames go above a certain threshold, then you have a potential Ransomware issue. Our recommendation is to base your alert on anything above 4 renames per second.

3. Create a sacrificial network share

When Ransomware strikes, it typically looks for local files first and then moves onto network shares. Most of the variants that I have looked at, go through the network shares in alphabetical order G: drive then H: drive etc…

A sacrificial network share can act as an early warning system and also delay the Ransomware from getting to your critical data. Use an early drive letter like E:, something that comes before your proper drive mappings. The network share should be setup on old slow disks and contain thousands of small random files.

When doing small random files, there's no easy way to get the list of files in the right order to avoid lots of seeking around the disk. Depending on how it is implemented, the cipher might need to be re-initialized for each file and thus slowing down the encryption process.

The slower the disk the better. You could go to the extreme and put it behind a router and limit data throughput to this network share. It may add a slight delay to the logon process but this honeypot may give you enough time to shut client machines down if they get infected with Ransomware.

You could also setup an alert which would trigger if a specific file was accessed somewhere within the network share. This would be a sure sign that something was going through your file shares. You just need to educate your users to stay away from this network share.

4. Update your IDS systems with exploit kit detection rules

Many IDS, IPS and firewall systems come with exploit detection features. Exploit kits are used as a way to get Ransomware onto a client through malspam or via compromised websites.

The two most common exploit kits (EK) associated with Ransomware are the Neutrino EK and the Angler EK. Check if your network security monitoring systems are up to date and see if they have the capability to detect exploit kits.

LANGuardian includes the Snort IDS system which supports the detection of exploit kits. Watch out for any activity in the *Top Network Events* report.

5. Use client based anti-ransomware agents

Over the past few months, companies like Malwarebytes have released anti-ransomware software applications. These are designed to run in the background and block attempts by Ransomware to encrypt data. They also monitor the Windows registry for text strings known to be associated with Ransomware. The problem with this approach is that you will need to install client software on every network device.

Researchers are also looking at ways to 'crash' computer systems when droppers are detected. Droppers are small applications that first infect target machines in preparation for downloading the main malware payloads. This will likely mean that the system is sent to IT where the attack should be discovered.

You should also inform your network users to avoid installing agents themselves. There is too much of a risk that they will install the wrong agent or they end up install more malware on their systems.

NetFort LANGuardian - proven by education institutions around the world

As illustrated, NetFort LANGuardian has been used by educational institutions around the world to effectively monitor the traffic flowing across their campus network. LANGuardian reports on the health and security of the network and records details of user activity and traffic volumes. It also features a number of customizable dashboards to enable a real time and unified visibility of campus network and user activity, making it easy to quickly identify unusual activity and perform instant drill down to the required level of detail (even at the individual user level) to understand exactly what is going on. LANGuardian also includes a built in database for historical reporting, forensics and trending.

For More Information:

To learn more about NetFort LANGuardian, to see LANGuardian in action, or to get a free 30-day trial, visit www.netfort.com or to discuss your specific networking needs with one of our campus networking experts, or request a live demo of LANGuardian, contact us at nasales@netfort.com.