TECH REVIEW 2014

Network Box technological news and articles over the last 12 months

- Entities
- Security Modules and Service Packages
- Network Box 5 Administrative Configuration Portal
- Network Box 5 User Interface Enhancements
- The Vulnerability of Everything
- Key Performance Indicators
- DNS Amplification (and other) Attacks
- Trust in an Unforgiving Cyber World
- Bash Vulnerability – Shellshock
- Cloud Mail Backup
- Frontline Protection and Infected LANs
- Event Correlation
- Cloud DNS Backup
Entities

Network Box 5 introduces the concept of entities. This article discusses what these are, how they are used, and how they can help you monitor and control the policies of the users and resources on your network.

The ‘user’ Problem

In the realm of gateway threat protection, it is notoriously difficult to determine what a ‘user’ is.

- Is it a workstation? But what if the workstation is shared and used by more than one person?
- Is it a logged in user? But what about servers (such as mail servers) handling messages for hundreds or thousands of different mail accounts?

Network Box 5 addresses the problem with the introduction of the concept of an entity.

The Entity Solution

Put simply, a Network Box 5 entity is either a shared server (a network entity) or a person/automaton (a user entity). You would typically create individual entities for each of your shared servers, as well as for each user account on your system.

Every network session that passes through the Network Box 5 device is then allocated to a set of 4 entities:

1. A local network entity
2. A local user entity
3. A remote network entity
4. A remote user entity

The terms ‘local’ means belonging to the protected network, while ‘remote’ means external. In the case where one of the four entities cannot be determined (or is not tracked), a special entity #0 (others) is used.

In this way, we can track the server the session came from, the server it is going to, the user at the remote end, as well as the user at the local end.

To illustrate, let’s look at an example:

Let’s say user Joe sends an eMail from his workstation to user Mary, delivered to the mail server.

1. A local network entity: Joe (his workstation)
2. A local user entity: Joe (the user)
3. A remote network entity: Mail Server
4. A remote user entity: Mary (the user)
Entity Attributes

To implement the entity system, Network Box 5 uses entity attributes. Each entity in the system is assigned an ID (a number) and is uniquely identified by a name. Entities can have one or more attributes assigned to it, and these attributes includes things such as:

- Passwords
- eMail addresses
- Host names
- IPv4 addresses
- IPv6 addresses
- MAC (hardware) addresses

Entity attributes are dynamically created and maintained by the system, both by synchronization (against such things as Active Directory or LDAP servers) and by learning behavior (based on transactions such as logins, logouts, DHCP allocations, verification, etc). In addition, entities and their attributes can be manually maintained and tuned from the administrative consoles.

What can be done with entities?

As each network stream is assigned to entities, and per-minute summary statistics are maintained on the network bandwidth used by entities, the first real use of entities is for reporting. With Network Box 5, you no longer need to report on network bandwidth usage by IP address, but can now focus on the users of the bandwidth.

As a result of the attribute system, you no longer need to worry how to group reports by user. A particular user may have multiple IP addresses at one time (for example his workstation, desktop VOIP phone, as well as mobile phone and tablet on wifi) – but each of these are attributes of the user’s entity, so are automatically grouped by that user.

The entity system becomes a large on-the-box cache of information about the users of the network. Once built-up, this can be used for a multitude of security functions. A good example is envelope verification (verifying incoming eMail RCPT TO email addresses against the email attributes of entities on the system, and refusing email to non-existent addresses).

Entities can be used for problem tracing. When the user calls up complaining of a problem he is happening, the administrator can call up information on all that user’s activity, across all his devices, and show all policy control blocks for that user (regardless of device or location).

And, entities can be used for control. The policy rules can now control entities, irrespective of the device they are associated with.

Summary

In summary, the entity system in Network Box 5 provides for grouping the activity of all the devices in your network, and assigning that activity to individual users. Comprehensive reporting and policy control facilities are then made available – all based on the users, not IP addresses, of your network.
The Network Box 5 product is delivered as a set of security modules building upon a single base module. The base module consists of a kernel, user space toolchain, logging and configuration – essentially an extremely sophisticated router – and it is these security modules that provide the security functionality. The security modules are inter-related and communicate amongst themselves, but each individual security module is targeted towards a single security problem. Examples of such modules include:

- Web Client protection
- Web Server protection
- SMTP Mail Server Protection
- Anti-Virus scanning
- Intrusion Detection
- Quality of Service

As you can see, some of these modules provide specific security functionality (such as anti-virus scanning) and are used as tools by other higher-level modules. Other modules provide specific protection (such as web client protection). An important distinction is drawn between client and server protection – even if the core protocol (e.g.; http for web) is the same, the threat landscape and protection requirements are completely different.
Network Box 5
Service Packages

Service packages are bundles of security modules. In general, it is more cost-effective to choose a service package, than a group of individual security modules, as bundle pricing is available for service packages.

The core four Network Box service packages based on “scanning technology” are still available and offered in Network 5:

- **FW+**
  - Firewall Plus
- **AV+**
  - Anti-Virus Plus
- **CF+**
  - Content Filtering Plus
- **UTM+**
  - Unified Threat Management Plus

And in addition, a fifth such package is now also offered to provide for Web Application Firewall protection for web servers:

- **WAF+**
  - Web Application Firewall Plus

But, now we also offer the option for application-based service packages:

- **EMP+**
  - eMail protection
- **WBP+**
  - Web Browsing protection
- **FWAF**
  - Firewall+ and WAF protection bundle
- **UTMW**
  - UTM+ and WAF protection bundle

For example: if your goal is to protect web clients, you may find the WBP+ package more suitable than CF+, as it includes both anti-virus and content filtering protection for web clients.

Network Box 5
Optional Security Modules

Network Box 5 also includes a number of optional security modules. These can be chosen either to add on specific optional security technologies, or to supplement a service package with additional functionality. Examples include:

- **NAVL Application Identification**
  - (1,000+ applications identified)
- **Data Leakage Prevention**
- **Clustered Scanning**

Conclusion

Network Box 5 takes the four core service packages of Network Box 3 and provides alternative choices for application-based service packages and optional security modules. Each security module is targeted towards a single specific security problem.
Network Box 5
Administrative Configuration Portal

The new Network Box 5 web-based administrative configuration portal allows users to configure and control their network settings. In this article we will highlight some of the key components of the Administrative Web Interface.

User Configuration in Network Box 5

When you enable the Administrative Web interface in Network Box 5, you will now notice two new tabs: Configuration and My Account.

▶ The Network Box 5 web-base administrative configuration portal allows users to configure their network settings.
Configuration Synchronization and Visibility

Network Box 5 offers a full bi-directional synchronization of configurations between the BOX and its SOC, as well as a unified configuration language. The first change you will notice is that the entire configuration of the box is now shown in the Overview section of the Configuration tab. A dramatic improvement over what was possible in Network Box 3, this allows for a simple copy-and-paste to document the configuration in audit reports. It also allows the customer to see the changes reflected in the configuration as a result of change requests to the SOC.

Content Filtering

The content filtering configuration system allows URLs to be re-categorized, and customer web content filtering rules to be designed and applied to the box policy.

Access Control Lists (ACL)

A generic access control lists feature is present to allow typed lists of things such as IP addresses, eMail addresses, Content Filtering categories, etc, to be maintained. These ACLs are then used in other parts of the configuration.

Anti-Spam

The anti-spam configuration system allows rules to be created to whitelist and blacklist eMails for the anti-spam system.

My Account

The My Account tab is available to allow the administrator to maintain his own account (including such things as password and notification preferences). Other administrator accounts can be maintained via the entity management system in the Configuration tab.

Entity Configuration

A web-based user entity configuration system is now available to allow entities to be created, and their attributes to be manually maintained (if necessary) or merely viewed. An example use of this would be to set a password for an entity, or to assign the entity a vpn attribute to allow the user to connect via VPN.

Conclusion

The web-based administrative configuration screens are designed to provide equivalent, but more flexible and powerful, functionality to that provided by the Network Box 3 platform. These are provided to help with customers migrating from Network Box 3 to 5. However, more configuration functionality will be released – in particular control functionality to allow for administrative control of such things as services, connections and VPN links.
Network Box has been releasing an average of 100 fixes and improvements to our Network Box 5 product each patch tuesday. These have included new security modules, new information screens, as well as performance and other enhancements. With the May 2014 patch tuesday, this trend continues. In this article we will look at three in particular: Bandwidth Display, VPN Status Display and Holistic Search.

Bandwidth Display

Both Network Box 3 and 5 have for some time now been able to show you how much bandwidth you are using - both on a per-interface as well as per-user basis. However, Network Box 5 takes this a step further by requiring the specification of how much bandwidth you have available, as well as classes of interface (such as Internet, DMZ, VPN, etc). This allows us to show bandwidth usage as a percentage, as well as use it as a centralized control for such things as Quality of Service, traffic re-queuing and packet prioritization.

To further improve the visualization of this, we have introduced a dedicated screen to the Administrative Web Portal (Analysis / Network / Bandwidth). This new screen shows the average and peak bandwidth usage of each of your Internet links. It charts both receive and transmit bandwidth, as well as shows you the top applications on your network.
VPN Status Display

While Network Box 3 could display some VPN status information, it was not unified in any way. With Network Box 5, we have unified all VPN types (IPSEC, SSL, PPTP, etc) into a single unified framework, and centralised status, reporting and control. We’ve also taken the opportunity to include geographic attributes to the VPN end-points, to allow us to know (and display) the geographic path of each VPN link.

We introduced a new screen to the Administrative Web Portal (Analysis / Module / VPN). This new screen shows the status of each of your VPN links, both as a table as well as a real-time map.

Holistic Search

We have spoken about the holistic entity system at the core of Network Box 5, and how it allows you to group all a particular user’s devices and activity under one single holistic entity (for control, display and reporting purposes). I’ve also spoken about how this system can be used to ease the administrative burden by allowing you to display the activity for a particular user, centrally, irrespective of which device or application the user is using.

We have brought this powerful facility front-and-centre by including a holistic search box right on the front page of the Administrative Web Portal. Enter an IP address, eMail address, or any such attribute, and the system will immediately display a summary of the recent network activity. Searches can be further refined by selection from 19 available attributes (including such things as country, city, threat, application, etc).

Conclusion

Network Box will continue to refine and improve our Network Box 5 product and deliver those updates to you automatically every patch tuesday - all as part of our service to you.
Businesses are now facing cyber threats, via vectors, which just a few short years ago, would have seemed like something out of a Hollywood science fiction movie, or a particularly inventive television episode of, ‘Mission Impossible.’

The Vulnerability of Everything
by Michael Gazeley

When you plug into the world, it’s easy to forget the world is also plugged into YOU

Risk Management, in a business context, is defined as the forecasting and evaluation of financial risks, together with the identification of procedures to avoid, or minimize their impact. But how can ‘management’ be made to understand, manage, and mitigate today’s cyber risks? Unfortunately, outside of the IT Department, most managers simply don’t understand, (or don’t want to understand), the very real-risks posed by cyber-threats. And IT Managers often don’t have the influence required to force through much needed changes, in both corporate thinking, and corporate spending, on cyber security.
Recently, 40% of the population in South Korea had their personal details stolen.

How bad do things have to get, before people sit up and take notice? In the world today, we are faced with smart phones and tablet computers, which can bypass an organization's firewall, if the office network is not setup securely. Not only that, but in that office, more and more smart 'connected' devices are being installed, often without any planning, resulting in office printers, fax machines, telephones, video surveillance, web cams, and copiers, which can be leveraged to both spy inside the office network, as well as attack third-parties outside the office network.

One million new devices are being connected to the Internet every 3 hours.

Examples of such attacks, range from the almost comical discovery that a Samsung refrigerator, which was compromised, and had become part of a spam bot-net. (It had sent out more than three-quarters-of-a-million spam emails, before the breach was discovered.) To more sinister examples of IP Teleconference Phones being hacked, to spy on organizations' board meetings. And far worse than that, hacked webcams (and even baby monitors!), used to spy on people (and their children) in their homes.

By 2020, there will be more than 50 billion devices connected to the Internet.

One of the largest recent successful cyber-attacks, on the retail sector, is believed to have been made possible by a security breach of the victim's Heating and Ventilation systems. Researchers have since discovered over 55,000 such HVAC systems connected to the Internet, and have noted that in most cases, these systems contain basic security flaws. Not to mention the fact that, "the security at such companies tended to be poor, and that vendors often used the same password across multiple customers."

Medical equipment such as surgical and anesthesia devices, pacemakers, insulin pumps, and lab analysis tools, can all be hacked.

The stark reality, is that major corporations and government departments, are moving at the speed of corporate red tape. While hackers and criminal organizations, are moving at the speed of the Internet.

It doesn't take much to realize who has the upper hand right now. And one shouldn’t forget the other unfortunate reality, which is the fact that the potential victim needs to successfully defend themselves from a never ending onslaught of attacks; while the hacker only needs to successfully get in once.
Yet despite all these facts, and despite the ever growing number of media headlines, highlighting successful attacks on companies and governments right across the globe, most senior managers are still all but ignoring cyber threats.

Sometimes it seems that the bigger the successful attacks are, often counting breaches of personal data accounts in the multi-millions, the more numb the entire world seems, to the shocking realities involved. And while you can usually change your password fairly easily, you can’t as easily change your social security number, or passport number, or your home address, or your mobile phone number. As the number of successful breaches grow, we are all becoming more vulnerable, as the criminals get a clearer and clearer picture, of our personally identifiable information.

Unfortunately, time and again, organizations are only looking seriously at their cyber security, after they become a victim of a cyber-attack. Sometimes, not even then.

This is simply not acceptable anymore. You cannot get your company’s private data back, once it’s gone. You cannot easily regain your clients’ trust, once their personal details have been stolen. Money stolen via on-line attacks, is just as real, as money stolen out of an armored car.

Cyber-attacks can, and do, cause very tangible damage, in the real-world.

There’s no time to waste, get properly protected today.

“You cannot escape the responsibility of tomorrow by evading it today.”

– Abraham Lincoln
In the business world, organizations worldwide have therefore come to rely Key Performance Indicators (KPI), which have become the standard method for measuring progress towards predefined and measurable goals. By using KPI throughout an organization, one can (for example) ensure sales are really up, costs are really down, quality is really increasing, and success is both real, and most importantly, repeatable. Without KPI in the workplace, it’s almost impossible to know what is going well, and what is not.

For all of these reasons, the Network Box 5 monitoring and reporting systems, have been enhanced to leverage the concept of KPI, for use in Managed Cyber Security.

By using KPI, each Network Box hardware appliance (or virtual device), is able to much better communicate what has been happening both in real-time, as well as over any given period of time. This spectrum of empirical information covers both the Network Box system itself, as well as the protected client gateway and computer systems in general.
Everything from network utilization, to how many web client requests have been made, to how many emails have been denied, to the average and peak CPU utilization, are carefully monitored and logged, to allow for detailed, fully customizable, real-time HTML-5 dashboards, and Adobe PDF format reports.

It is also possible to output this data to centralized organizational syslog servers, or to save it in various industry standard formats, such as comma-separated values (CSV).

In order to remove any initial learning curve, each Network Box 5 device (physical or virtual), comes with pre-defined KPI weekly reports, which closely mirror the weekly reports which have always been part of the Network Box 3 managed security services. The inclusion of a default report will allow any Network Box 3 client to upgrade to Network Box 5, without immediately needing to lean about the new KPI systems built into Network Box 5.

Once upgraded to Network Box 5, a standard (default) Network Box KPI weekly report will be delivered, in place of the old Network Box 3 weekly report.

However, given the enormous power and flexibility of the new Network Box 5 monitoring and reporting systems, it is obviously well worth utilizing the new built-in KPI capabilities to produce bespoke real-time HTML-5 dashboards and periodic Adobe PDF format reports.

The objective of Key Performance Indicators in general, and the new Network Box 5 KPI monitoring and reporting systems in practice, is to at least allow IT Managers to turn the car headlight back on, and allow them to look out of the front windscreen.

There are twenty one initial Key Performance Indicators offered by the new Network Box 5 KPI monitoring and reporting systems.

1. Network (INTERNET) utilization
2. Network (LAN) utilization
3. Network (DMZ) utilization
4. Network (VPN) utilization
5. DISK utilization
6. CPU utilization
7. Network Firewall connections denied
8. Web Client requests made
9. Web Client requests denied
10. Web Client URL categories
11. Web Client Threats
12. eMails received
13. eMails denied
14. Outgoing eMails sent
15. Outgoing eMails denied
16. Incoming eMails received
17. Incoming eMails denied
18. eMail SPAM blocked
19. eMail MALWARE blocked
20. eMail POLICY blocked
21. eMail DLP blocked
For each of those, there are six variants:

1. 24-hour average
2. 24-hour peak
3. Peak-hours average
4. Peak-hours peak
5. Off-peak-hours average
6. Off-peak-hours peak

These allow for a total of one hundred and twenty six KPI which can be monitored and reported on as required right now.

In the near future we also plan to release the following KPI types.

1. VPN SSL site-to-site connections made
2. VPN SSL client connections made to the server
3. VPN SSL site-to-site percentage uptime
4. VPN PPTP connections made
5. VPN IPSEC connections made
6. VPN IPSEC percentage uptime
7. Frontline IPS attacks denied
8. IPS attacks denied
9. IDS attacks detected
10. WORKLOAD utilization
11. MEMORY utilization

This will bring the total number of KPI to one hundred and ninety two, as all of the KPI types will be available in six variants.

For each KPI, as an overview, it is also possible to make a comparison between any two defined time periods. This facility is very useful to see if workloads are increasing over time, for example, to see how many more emails are being scanned by the system this week, than in the same week last year.

1. Current time period (day, week, month, etc)
2. Previous time period (previous day, week, month, etc)
3. Percentage change from previous to current

For each KPI, in detailed view, provision is also made to show:

1. KPI history over time (chart/table of KPI over time, to see historical trends)
2. KPI Statistics (for each time period, the average of the KPI)
3. KPI Tops (depending on the KPI, but things like Top Users, Top Senders, Top Recipients, etc)
The Domain Name System (DNS)
The Domain Name System (aka DNS) is the Internet facility primarily responsible for converting name (www.network-box.com) into IP addresses (218.213.64.30 and 2001:db0:a5::18). It can also be used to store textual records, mail routing records, and other information. Applications using DNS typically connect over UDP port 53, although TCP port 53 is used as a fallback for large records as well as bulk information transfer. Being based on UDP means that the protocol is vulnerable to spoofing attacks (where the sender IP address is not real, but is spoofed to look like someone else), and this is indeed where most of the problems are based.

DNS AMPLIFICATION (and other) Attacks

The Network Box Security Response monitored an increasing number of DNS Amplification Attacks both targeting, as well as attempting to leverage, our customers’ DNS infrastructure. This article gives some background information on these attacks, along with advise for how to survive.

www.network-box.com
Open DNS Servers
The core problem, and first to address, is that of ‘open’ DNS servers. DNS requests typically fall into one of two categories: authoritative and non-authoritative, and the issue is one of recursive lookups to non-authoritative DNS servers.

1. In the case of an authoritative request, a DNS request for a particular domain name is sent to the server directly responsible (authoritative) for that domain name - the response is said to be ‘authoritative’ because the DNS server represents the authority for that domain and the DNS clients need look no further.

2. In the case of a non-authoritative request, a DNS request for a particular domain name is sent to a server not directly responsible (not authoritative) for that domain name. In such cases, the server can do one of two things - it can either refuse the request, or it can go ahead and look up the domain (recursively) on behalf of the client.

The problem comes from DNS servers that are publicly available and configured to allow recursive requests from public (non-trusted) clients. If your DNS server is configured in such a way, then remote untrusted users can use your server to lookup other people’s domains. More importantly, remote malicious users can use your DNS server to attack other people’s DNS servers over the Internet. The problem is very similar to that of third-party-relay with SMTP email.

I cannot stress enough how important locking down the configuration of any publicly accessible DNS servers is. It is no longer a matter of “if”, but more “when” your DNS server will be leveraged by someone malicious to attack someone else, and you will get the blame. Statistically you are vastly more likely to be leveraged as the source of an attack, than to be the target of such an attack, but both have equally disastrous impact on your network service availability.

Mitigation Technique:
Custom IPS rules can be enabled at the perimeter Internet Threat Protection device, to deny recursive DNS lookups coming from untrusted public IP address ranges. Rate limiting can also be used, per source IP (even spoofed).

DNS Amplification Attacks
A typical DNS amplification attack involves the attacker sending a DNS lookup request to an open DNS server, but spoofing the source address to be the IP address of the target. Often, the "ANY" resource type is requested, to return a large amount of information in the response, and the response packets quickly overloads the target server. Such attacks levels open DNS servers, so cannot leverage you if your DNS server is not open to recursive queries. You can still be the target of such an attack.

Mitigation Technique:
Custom IPS and firewall rules can be enabled at the perimeter Internet Threat Protection device, to deny DNS replies as the first packet of a new network connection. Custom rules can also be enabled to detect and block the most common known such DNS attacks (often based on threshold limits for aggressive response).

Conclusion
Longer-term, there are efforts underway to secure the underlying DNS protocol, but those are many years off and will require extensive upgrades to the DNS infrastructure. Short-term, the best solution is to make sure you are not part of the problem by disabling recursive lookups on your public-facing DNS servers, and to make sure you have protection in place so that you can mitigate the attack if you are targeted.
TRUST

In an unforgiving Cyber World

by Michael Gazeley

Reputation (or trust) based cyber security systems, are growing rapidly in popularity, for the simple reason that they work. They add an additional layer of much needed real-time protection, against the rapidly changing cyber threat landscape.

Instead of just relying on the scanning of data packets at the gateway, these reputation systems allow additional judgments to be made, some based on contextualized data about the files being scanned, and some based on where the data packets being received actually came from.

Such logic, of course, isn’t new.

Financial institutions, have been relying on credit scores to make decisions about lending money to people and businesses, for a very long time. Corporations offering potential key hires important (or sensitive) jobs, often rely on background checks performed by trusted third-party organizations. And increasingly, airport security services around the world, are starting to look at travelers’ histories, long before they even turn up at the ticket counter.
These are all reputation (or trust) based approaches, to real world security problems.

Organizations around the world, need to ensure that their vital business communications, can rely on data only going to and from trusted sources. Malware, SPAM, Phishing Emails, and other cyber threats, have grown exponentially over the last few years.

Advanced Threat Intelligence, is key, to dealing with Advanced Persistent Threats. Therefore, making the very fullest possible use of trust based systems and technologies, is vital.

The Network Box 5 Managed Security Services Platform, leverages an increasing number of reputation and trust based systems. Some developed in-house by our programming team, who have won more than 80 industry awards over the last decade, and others from world-class security partners and providers. The technologies involved, go well beyond that of a ‘simple credit bureau approach’ to trust, and integrates up to seventy-eight security engines, which are either updated using Network Box’s patented high speed PUSH update technology, or Network Box’s (even faster) multi-award winning Z-Scan cloud based cyber defense shield.

The augmented gateway security on offer with Network Box 5, takes the new systems’ capabilities far beyond what is possible using Network Box 3 based technology.

Network Box 3 based systems, have done an absolutely amazing job over the last seven years, but the Network Box 5 platform is built for the future. The Intrusion Detection and Prevention systems built into Network Box 5, for example, are able to fully utilize the multi-core architecture of the CPUs in the latest hardware, to deal with emerging threats in the most efficient manner possible.

Once reputation security is implemented however, it is almost inevitable that some of the individuals, companies, and organizations which one deals with, will turn out to have a reputational issue, at least in cyber security terms.

It may be that a supplier's organization has been blacklisted as a spammer. It may be that a vendor's website has become compromised, and is now infecting visitors. It may even be that an important customer's network, has become part of a well-known botnet.

Security organizations are leveraging ‘reputation,’ to secure networks in a highly scientific way. Hackers, malware writers, and spammers, on the other hand, are leveraging ‘reputation’ in a highly emotional way, to try and compromise those very same networks.

The bottom line is that despite the fact you may know, and therefore personally trust, the victims who are the source of these cyber threats, that does not make the threats any less real. Indeed, the potential threats are all the more dangerous, because they are either really from ‘trusted’ sources, or appear to be from ‘trusted’ sources.

So the next time a supplier’s email gets blocked because their network is blacklisted, be careful not to whitelist them too broadly, or you could end up drowning in SPAM. If you visit a website you go to everyday, and it’s suddenly blocked because it’s listed as compromised, realize that it is almost certainly hacked and infected. And if you have an email blocked, because it has been sent from a network which is listed as part of a highly dangerous bot-net, don’t be of the mindset that just because it’s from your best customer, that you can simply ignore the warning.

In today’s unforgiving cyber world, safe is definitely preferable to sorry.
On the 25th September a vulnerability in the bash shell, commonly used with Unix/Linux products, was announced and given the identifier CVE-2014-6271. The vulnerability proved to be extremely exploitable, and both security researchers and malicious agents started to mass scan the entire Internet looking for vulnerable servers.

Almost immediately upon the public release of patches, security researches started to question the effectiveness and completeness of the official fixes. Sure enough, a subsequent vulnerability (CVE-2014-7169) was announced, documenting a new way of exploiting even patched systems.

Network Box Security Response announced Threat Level 4 (to put that into perspective, we had not been at that level, for this serious a vulnerability, since 2006), and a lot of sleep was lost providing patches and protection signatures against all the scanning and exploit activity. The popular name ‘shell shock’ was given to describe this new threat - and it was an apt name, given how many in the security industry felt after the first 24 to 48 hours of dealing with the fallout from this new threat.

What is Bash Shellshock?

So, what is bash Shellshock, and the CVE-2014-6271 and CVE-2014-7169 vulnerabilities?

Simply put, the bash shell has a facility whereby functions (executable commands) can be put into environment variables, and when a new bash shell is executed with that environment, it executes those commands. The vulnerability is that if an attacker can control what goes into environment variables, and if the vulnerable program executes the bash shell, then the commands will run (with the security credentials of the program executing bash). This is a classic remote-exploit.
A simple example to show the vulnerability at the command line is:

```bash
env x='() { :;}; echo I am vulnerable' bash
```

That sets the environment variable `x` to the value `'() { ;}; echo I am vulnerable'`, and then executes the `bash` shell. The result is that "I am vulnerable" is printed on the console.

Note that the vulnerability is actually more accurately described as that the executable commands can be put after the function definition, but from the attacked system’s point of view it makes little difference.

The reason that the issue is so serious is because it turns out that it is not difficult to get arbitrary data into environment variables. For example, the popular CGI scripting system (used by an enormous number of public-facing web servers) will put the headers provided to the web server into environment variables, prior to executing the CGI script. Exploit is as simple as setting the user agent in the web request to be the exploit code. The only thing stopping exploit is then whether the CGI script actually executes the `bash` shell.

Some DHCP clients also appear to be similarly vulnerable (they put options provided by the DHCP server into environment variables, prior to executing `bash` to configure the network interface), and more and more possible exploit vectors are being found each day.

**Current Situation**

The current situation for Network Box customers is that we have released (and continue to release) NBIDPS and WAF+ signatures to protect against exploit. We continue to see extensive scanning activity (both malicious and reconnaissance), although this has died down in recent days.

However, it must be pointed out that gateway-level protection is only one part of a defence-in-depth strategy. While we can protect against known exploits, vulnerabilities such as this have proven in the past to be exploitable in new and inventive ways - and sometimes those exploits come from within the network (not even passing through the gateway). The DHCP vector is particularly concerning.

Now that full comprehensive patches have been released by the vendors, and those patches address both CVE-2014-6271 and CVE-2014-7169 vulnerabilities, Network Box Security Response has been working with local NOCs and customers to actively patch potentially vulnerable servers. We continue to recommend and strongly encourage customers to conduct an internal audit to enumerate potentially vulnerable systems, and to ensure that those systems are patched.

Given the state of our signature protection, and patch levels of our customer base, Network Box Security Response last night lowered our alert level to 3, and will consider further lowering it in the coming days.

**The Future**

The biggest concern with these vulnerabilities is that they will be exploitable by a network worm. Should a large number of vulnerable systems remain un-patched, and a mass exploitable vector be discovered, that remains a very real possibility. The only way to comprehensively protect against this is by ensuring potentially affected systems are patched. There are a very large number of embedded and other such devices running Linux.

For our customers, Network Box Security Response continues to closely monitor the situation and refine our signature protection to address new and emerging variants of these exploits.

www.network-box.com
In the case of Microsoft Windows based email servers, which require regular updating, patching, and rebooting, the email queuing system on Network Box 3, is a great way to prevent business interruptions to incoming emails, with senders not even being aware that the clients’ email systems was down at the time of reception.

However, there are certain circumstances where the Network Box 3 email queuing system is not able to help. Examples include problems with Internet connectivity, power-cuts, faulty switches, or bad cable connections. Essentially, if the fault is behind the Network Box 3 email queue, it can help. If the fault is either in front of, or includes the Network Box 3 system, then it cannot help.

Network Box is pleased to announce the global launch of our Network Box Cloud Mail Backup system. This Network Box 5 based, cloud email queuing system, is a very significant upgrade to the local (appliance based) email queuing system, which is an existing part of Network Box 3.

Email queuing on the Network Box 3 platform, has always been an extremely popular feature. This built-in business continuity system, helps to mitigate the risk of emails being ‘bounced,’ or otherwise lost, due to issues with clients’ email servers.

In the event of a client's email server having a problem, regardless of it being a hardware failure or a software fault, as long as the email server concerned is unable to receive emails, the client’s Network Box 3 system will store and queue up the undelivered emails on its local hard disk drive, ready to automatically deliver them, as soon as the issue with the client’s email server has been resolved.
• Clients will have full control over which of their domains will use the service.

• Clients will have full control over which cloud backup servers will be used to back up their mail, so that their email never leaves a certain geographic region. For example, to meet local legal requirements.

• In the event the primary MX servers cannot be contacted, if so configured, the client's email will be redirected to, received by, and stored on the cloud backup servers. These servers will periodically, and repeatedly, attempt to deliver such email to the primary MX servers, and will queue the emails until such time as delivery is successful.

• Once delivered, the email will be removed from the cloud backup servers, and only logs (containing date, time, sender and recipient) will be retained.

• Only email current queued for delivery to an unreachable primary MX server, will be stored on the cloud backup system, and such emails will only be stored on servers explicitly designated as to be used by the customer in his DNS MX records.

• This backup queuing will also occur if the primary MX servers are overloaded and temporarily not accepting new connections / emails.

• Should a particular cloud backup service be unavailable for any reason, it will not provide mail backup services, and will not redirect mail to an alternative geographical region.

• Only inbound mail backup service is provided.

• The cloud backup servers will not accept or queue any emails larger than 10MB.

• The cloud backup servers will not issue any NDR (Non-Delivery-Receipts).

• The cloud backup servers will queue emails for a maximum of 5 days.

• No SMTPS service is provided.

• No recipient verification is attempted other than the domain check.

In contrast, the Network Box 5 based, cloud email queuing system, can help mitigate problems with receiving emails, regardless of where the local fault resides. The Network Box Cloud Mail Backup system operates independently, in the event that a client has a local issue impacting the reception of email at their email gateway.

This new in-the-cloud mail queuing facility, allows all email to be backed up in the cloud, so if there is a problem with the ISP, the internal network, or the email server, the mail will be stored in the cloud, and delivered when the problem is resolved.

In order to ensure maximum resiliency, Network Box has deployed a globally distributed set of high speed cloud servers that act as backup MX (Mail eXchange) servers, for customer SMTP mail.

It is possible to define exactly which email domains will enjoy this cloud backup service, using a new 'Box Office' configuration system. 'Box Office,' will also give an overview of the current status of the cloud mail backup system. In addition, an on-the-box overview of the current status of the cloud mail backup system will be available, on the HTML-5 Dashboard.

This is a FREE SERVICE provided to all Network Box 5 customers subscribing to our various Managed Security Services that include email scanning, such as our AV+ and UTM+ services.

At any given time, the current status of cloud mail backup for a particular customer can be checked in 'Box Office,' by looking at the owner account, 'Cloud Mail Backup Domains' section. (This is typically updated once a minute.)

This is the first of many cloud services that Network Box will be launching. The intent of this work is to offer improved security, functionality, and business continuity, by leveraging cloud technologies, to improve on what we can offer Network Box clients around the world.
Frontline Protection and Infected LANs

Network Box released enhancements to two core Network Box 5 modules – network-frontline and network-infectedlan.

network-frontline security module

Addresses the issue of front-line protection against scanning and intrusion activity. While higher-level modules (such as network-firewall, and network-ips) provide advanced protection using a huge number of signatures, network-frontline uses heuristics and a relatively small number of specifically targeted signatures to provide front-line protection with very little performance impact. Network-frontline is designed to be able to run on every Network Box 5 system.

Network Box released a new framework for our network-frontline security module in Network Box 5. This framework allows for highly configurable:

- Identification of scanning behavior from the Internet, by heuristic detection of protocol and port scanning rates.
- Highly-granular detection of non-protocol-conforming scans from known scanning engines.
- Standardized support for tripwire ports – particularly useful for detection of slow scans.
- Optional support for dynamically blacklisting detected scanners.

network-infectedlan security module

Addresses the issue of identifying infected workstations and servers in the LAN / DMZ areas of your network. While higher-level modules (such as anti-malware and content filtering) can detect access to malicious content, the network-infectedlan module attempts to identify outbound botnet access from your network. Again, it is very lightweight (performance wise) and designed to be able to run on every Network Box 5 system.

Network Box released a new framework for our network-infectedlan security module in Network Box 5. This framework allows for highly configurable:

- Detection of outbound access to known public botnet command and control servers.
- Detection of outbound access to known malware update sites.
- Highly-granular detection for highly-prolific malware (such as Palevo, Conficker, Zeus, etc, for example).
- Optional support for dynamically blacklisting detected infected workstations/servers.

Note: To support those of our customers using Network Box 3, we have back-ported what we can, and we also released some parts of the network-frontline framework for the Network Box 3 platform.

Together both these modules provide highly effective, but extremely lightweight (from a performance point of view) protection for both inbound intrusions as well as infected workstations/servers connecting outbound.
One of the most common requests we receive at our Security Operation Centres is when customers ask us to notify them if there is an intrusion attempt against their network. The issue we have with this is twofold:

1) Our primary mission is to protect our customers. That means that our primary focus is Intrusion Prevention, not just Detection. We stop the attack, not just let it through and then tell you about it later.

2) Every minute of every day, the public Internet is scanned – from thousands of sources in hundreds of countries. They respect no network or international boundaries, and the scanners try to get into your network. Some of these scans are truly malicious, some are configuration mistakes, and some are purely for research purposes. Most are automated, but all are an intrusion attempt into your network. We call this Internet Background Radiation.

Alerting on each and every one of these intrusion attempts would mean alerting dozens of times every hour on even the smallest of networks.

For Network Box 5 customers, we released our Event Correlation system. This new system correlates intrusion activity across all the network-frontline, network-ips, network-ids and network-firewall systems. For each source IP, it maintains statistics on the number of targets hit, the number of blocks seen, the number of scans seen, and the number of different types of attack seen. The system is highly configurable, and thresholds for each of these four attributes of an intrusion can be set, in order to escalate the intrusion incident for further processing.

Escalation options include:

- Dynamically blacklisting the source of the attack, usually for a small number of minutes (sufficient to interfere with the attack).
- Alerting (via eMail) administrators as to the source and details of the attack. An alert is raised both when the attack is first seen, as well as when it is determined to have finished.

With this event correlation system, the number of alerts raised can be dramatically reduced (removing most of the noise of Internet Background Radiation). However, while the size of intrusion necessary to raise an alert can be configured, this system is still likely to raise several alerts each day (for small networks) and hundreds of alerts each day (for large networks). The sad reality is that there is so much malicious scanning and automated intrusion activity on the Internet every day. For this reason, we don’t recommend that this alerting mechanism be generally enabled – but it is available for customers who need it.

Remember that our primary mission is prevention of the attack, and the dynamic blacklist facility, based on event correlation, provides an excellent tool to interfere with external network scanning and intrusion activity.

To support those of our customers using Network Box 3, we also released our event correlation and alerting system for the Network Box 3 platform, as well as Network Box 5.
After we launched our Cloud Mail Backup service, we have been rolling this out globally to our Network Box 5 customer base. Since then, we’ve also added a country-level cloud backup centre in Germany (which provides the option to keep the eMail within Germany for those European customers with privacy concerns).

As we promised then, Cloud Mail Backup was just the first of many cloud services to be launched, and we are pleased to announce the launch of our second cloud service - Cloud DNS Backup.

A DNS Server on the Box

We released a DNS recursive resolver to the Network Box 5 platform. Based on an enterprise-grade DNS server, this allows the box itself to recursively resolve DNS queries itself (without relying on external recursive resolvers, and able to operate off the root level DNS servers themselves). This service can also be offered to workstations and servers on the LAN/DMZ (so such machines can use the Network Box at the gateway as their specified DNS server).

Building on that, we’ve also released an optional network-dns-server security module. This security module provides the capability to configure DNS zones as either master or slave, on the Network Box itself. The Network Box will serve queries to those zones in an authoritative manner.
DNS Servers in the Cloud

To further extend the capabilities of this system, we also released Cloud DNS Backup. This allows customers to use Network Box’s extensive network of cloud DNS servers to provide backup DNS in the cloud. By using such a cloud based network, service reliability can be improved and DNS queries can be responded to, from the cloud, even if the Internet link to the master DNS server in the LAN/DMZ is down.

As with Cloud Mail Backup, the customer has full control over which Cloud DNS servers in which regions and countries, should be used to provide the service.

At any given time, the current status of Cloud DNS Backup for a particular customer can be checked in ‘Box Office’, by looking at the owner account, ‘Cloud DNS Backup Domains’ section. (This is typically updated once a minute.)

- Clients will have full control over which of their domains will use the service.
- Clients will have full control over which cloud backup servers will be used for their domains.
- In general, the DNS system operates with load-balanced round-robin behaviour. The selection of DNS server to be used to resolve a particular query is often random and unpredictable. It is important to ensure that all listed servers are authoritative and correctly configured for the domains they are serving.
- Only the DNS records themselves, as well as statistical logs, will be stored on the Cloud DNS Backup servers.
- Should a particular Cloud DNS Backup service be unavailable for any reason, it will not respond and the client will choose an alternate server to query (as per the standard mechanics of the DNS protocol).

This is a FREE SERVICE provided to all Network Box 5 customers subscribing to packages including our network-dns-server security module.

We plan to continue to release more of these optional Cloud services. The intent of this work is to offer improved security, functionality, and business continuity, by leveraging cloud technologies, to improve on what we can offer Network Box clients around the world.
Firewall
Intrusion Detection and Prevention (IDP)
Virtual Private Networking (VPN)
Anti-Malware
Anti-Spam
Web Proxy
Content Filtering
Data Loss Prevention (DLP)
Company Policy Enforcement / Compliance
Real-Time updates with PUSH Technology
Secure 24 x 7 x 365 Monitoring
ISO 9001 / 20000 / 27001
Certified Management
IPv6 Ready Core Phase-2 Certified
In-the-Cloud Protection
Comprehensive Adobe PDF Format Reporting
Apple iPhone / iPad HD Management Platform
Anti-Distributed Denial of Service Web Application Firewall
IPv4-IPv6 / IPv6-IPv4 Bridging
Multiple Internet Connections
High Availability / Load Balancing
Internet Acceleration
Secure VoIP (Voice over Internet Protocol) Gatekeeper
Secure Video Conferencing Gatekeeper
Quality of Service Control Traffic Policing
Denial of Service Protection Threshold Limiting
Hardware Fault Tolerance
Live Watch Real-Time Monitoring
Adobe PDF Report Generation
SSL (Secure Socket Layer) Virtual Private Networking
Anti-SPAM Pre-Scanning, bandwidth protection
Enhanced Image SPAM protection, including Optical Character Recognition technology
Mail Portal System, End User email management including SPAM release and white / black listing
Enhanced GUI (Graphical User Interface)
Secure Socket Layer (SSL) Proxy Application Identification
Entity Management
HTML-5 Dashboard
Cloud Mail Backup
Cloud DNS Backup

Network Box Corporation Limited
www.network-box.com

The trademarks, including but not limited to “Network Box” and the curly “N” device, are either trademarks or registered trademarks of Network Box Corporation Limited. Other trademarks and product names used in this publication are for identification purposes only, and may be the trademarks of their respective companies. Features and specifications are subject to change without notice. Benchmarking is performed with representative data, on a function by function basis. Weights and measurements are approximate only. Actual models may vary in appearance to the illustration and photographs provided.

Copyright © Network Box Corporation Limited 2015.