TECH REVIEW
2016

Network Box Technology News and Features
Long gone are the days when a computer virus would pop up a message on your screen “Your PC is now Stoned!”, or humorously display a trail of worms on your desktop. Today’s malware authors are mercenary in their approach, and primarily motivated by both the expansion of computer networks under their control and theft of your information. In particular, they are actively targeting point of sale units, credit card, user credentials, and other systems holding customer information.

In the words of Geena Davis (as Veronica Quaife) in the film “The Fly”, it is time to “Be afraid, be very afraid” and to take practical steps to lock down and secure such high value targets in your network. In most situations, in particular if you are already protected by Network Box equipment, you already have everything you need to do the job – you just need to get the policies defined, implemented, and ongoing monitoring in place. This article should give you some ideas and a plan to approach the problem – something we call the four I’s:

- Identify
- Isolate
- Implement
- and Incident response
Identify

Having recognized that this could be a problem affecting your organization, the first step is to identify the high risk target systems you have in your network. You do this by conducting a risk analysis of the information in your network, and the machines where that information enters, is stored, is processed, and leaves. Pay particular attention to customer private information, account information, credit card, point of sale, authentication, and banking systems (including those that store/use external bank authentication).

Such a risk analysis can be either conducted purely internally, or you can employ a third party consultant to assist. Both have their benefits and drawbacks – a third party consultant brings a fresh look at your systems, but doesn’t have the in-depth knowledge that your own team has.

Whichever your approach, the purpose of the exercise is to identify the systems of greatest concern so that specific protection mechanisms can be brought to bear. Security will always be a trade-off against convenience, but for these key high-value systems, the scales should always tip towards the side of maximizing security (even at the expense of sacrificing convenience). Risk assessment helps you identify the high value (to an attacker) systems, so that you can concentrate your efforts.

Isolate

Isolation is the technique of physically isolating these high-risk systems. It is not sufficient to merely partition these off as an IP address range, or run multiple subnets on the same physical wire. You need to physically separate these high-risk systems from the rest of your network.

The purpose of such isolation is to ensure that a penetration of your lower-value (perhaps easier to penetrate) networks, cannot cross across to your high-risk systems. Equally importantly, proper isolation ensures that you can implement restrictive policies to control the information flow not just into, but also out of such isolated networks.

Inter-connection of such networks to the Internet and/or internal systems is normally acceptable as a day-to-day requirement – but such interconnections must be via equipment that can control policy in a highly granular manner, and should normally include Intrusion Detection and/or Prevention technology to identify any pre-existing or new internal intrusion.

Be aware of dual-use equipment (for example, someone using a point of sale terminal for both taking money/credit card as well as normal web browsing or email activity). In general, such dual-use is frowned upon as it introduces unacceptable risk. Much safer to simply separate the functions, and keep the high risk information systems away from such high risk user activity.

Thankfully, nowadays, VLAN technology is robust, cheap, and easily implemented. Managed switches can uses untagged VLANs to implement such isolation, and tagged VLAN trunks connected to equipment such as Network Box threat protection devices to implement the policy control and Intrusion Detection / Prevention functions.
Implement

Once your high risk systems are isolated in their own network segments, it is time to design and implement the security policy for access to and from those segments.

You should always perform this from a deny everything, permit what is required, standpoint. Start by blocking all traffic into and out of these high risk networks, then identify what is required for day-to-day operation, and open up the policy to allow that specific traffic in/out. This policy needs to be as tight as possible. Here are some specific examples:

1. At the physical level, turn on ARP protection at your switch level, for those switch ports of servers and workstations connected to the high risk networks. Sure, it is slightly inconvenient when equipment is replaced/added, but the protection against ARP spoofing, combined with modern switches protection against passive network taps, is extremely effective.

2. At the firewall level, block everything then permit what is required. Connection tracking firewalls will allow you to do this with very fine grained control for most client-server network protocols today.

3.VPNs are an effective mechanism for imposing an access control layer on top of the usual network layers. But, put procedures in place to monitor VPN connections and be aware of malicious network activity bypassing firewall protections via VPNs. In general, we recommend that VPNs be terminated on the same equipment providing your policy enforcement functionality, and to subject the VPN traffic to the same policy control. VPNs should be used to increase security, not introduce backdoors to bypass protection mechanisms.

4. Assume nothing, and proxy/server locally whatever you can. For example, UDP/53 traffic that looks like DNS queries can leak information – so use an internal DNS server to host these and don’t permit UDP/53 outbound. Same for common services such as NTP, SMTP, etc. Application identification can help tremendously with this – just because it is port TCP/25 does not mean it is SMTP traffic.

5. Look closely at web traffic requirements, and lock it down as much as you can. Do you even need web browsers on this high risk equipment? Is it possible to just maintain a list of permissible websites, and block everything else?

6. Look closely at the requirements for such applications as eMail and file transfer. Can you block usage of those completely? Restricting the number and variety of outbound paths makes it simpler for you to monitor those remaining.

7. Consider the use of tripwire systems to detect scanning or other unusual activity within the network.

Once the policy has been implemented, turn on Intrusion Detection and Prevention systems and baseline the outbound network traffic. Then, setup alerts for anything out of the usual, in particular outbound.

Depending on your network, it may be possible to implement limits on network connection output volumes (again particularly in the outbound direction). Is it reasonable for connections to be carrying large volumes of data outbound?

Incident Response

The last step is to arrange an incident response system within your organization and your IT suppliers, including the Network Box SOC supporting you.

Understand the flow of incident reports, and arrange for monitoring of periodic reports from your protection systems. Make sure your escalation procedures are in place, and tightly controlled.

Summary

This four I’s approach to Identification of risks, Isolation of high risk systems, Implementation of effective policy control, and Incident response, is not new. What is new is the level and sophistication of malicious activity, and the extent.

The general approach you should be taking involves identifying the high risk systems within your network, and implementing special protection, policy control, and monitoring procedures to protect such systems.

There’s an old joke about a scuba diver asking a shop for the fastest fins that they sell. When asked why, he says that he is afraid of sharks. The salesman explains that he can’t possibly out-swim a shark no matter how fast the fins are. The diver replies that he doesn’t need to out-swim the shark – only swim faster than his buddy. Make your systems harder to penetrate than the other guy, and your attacker may just go elsewhere.
The general issue of security needs to be put into proper perspective – anything made by humans can, and will be, broken by humans; and in reality, those who break always have an advantage – they’re working with something that exists, and have the luxury of time to try and figure out how to break it. Whereas those who protect are in the opposite position – they’re always on the defense, they’re called to come up with new ways to create fences and perimeters that will withstand the constant assaults. Never has it happened in the history of humanity have defenses lasted through time.
Even the Great Wall of China, albeit still standing, in reality failed its purpose; it’s there simply because at some point it became useless, obsolete, so no one even bothered to attack it. Enough of philosophy though.

**Can we stop or prevent the attacks?**
No.

**Can we at least try to make their life difficult?**
We certainly can.

Unfortunately, the actual situation of cyber defenses is far from where it should be. Recent attacks on federal government data have clearly demonstrated that even those agencies are still ill-prepared to fend off attacks. It isn’t that they’re not doing enough; essentially, in many cases, they’re doing it all wrong. Many private companies, even today, are running firewalls that were obsolete 10 years ago, they’re not running IPS, they’re not running AV at the gateway, or web content filtering; they’re not scanning encrypted traffic. In a time when even a google search is encrypted, pretending that viruses can’t come through encrypted streams is 

![Hacked!](image)

I ask you, how many companies today are actually scanning for viruses at the gateway through encrypted streams?

I often have a hard time convincing my own clients that this is vital; they don’t want to take the time to do the setup necessary to implement such protections. They do not want to take the time to troubleshoot the few possible issues such implementation may bring about. Security takes time and patience, and not everybody is willing to put in the effort required.

Furthermore, many companies still try to do security on their own as if you could invent security expertise overnight; they don’t take security seriously, that is, until it hits them where it hurts – they lose something and, ultimately, they lose money and possibly the entire business.

As a managed security provider, we run into such situations every day. We acquire a new client, we analyze the configuration of their old firewall, and we realize there wasn’t even one. In this day and age, they’re still considering the LAN a trusted area, allowing all traffic outbound, opening ports right and left where it simply isn’t necessary. They’re still adopting security tactics that were already obsolete in 2002.

Attempting to do security without spending money, treating it as, well, as a nuisance. For as long as this continues, hackers will always have the upper hand.

**You ask if we can prevent or stop the attacks.**

**I would ask in return, can we ever hope to get ahead of the curve?**

Right this moment, we are left far behind, eating the dust. Hackers have basically demonstrated that if they want in, they’ll get in; period. To provide an idea of the extent of the issue, consider that we’re seeing more than 300,000 new threats per day. Think about that for a second; how many security people can you possibly ever hire to mount protection against 300,000 new threats every single day? AV companies themselves have lost the battle and conceded defeat long ago. They’ve been trying to create new technologies that could recognize threats without having to create signatures. In fact, many experts believe signatures are obsolete, and I tend to partially agree with that statement.

I say partially because signatures are still useful in recognizing existing, well-known threats. Imagine if we threw away all antibiotics because they can’t stop that new bacteria we’ve detected but then you get strep throat and you can’t be cured? Existing signatures are still very pertinent, to ensure that known and well recognized threats don’t destroy your network. For as much as there are 300,000 new threats every day out there, there are also more than 1.5 million well-known threats that CAN be stopped by an AV. We don’t pay much attention to them because the AVs are stopping them; but I assure you if we removed the AVs, those threats would join the legions of new threats and become a horrendous nightmare for us all.

**The state of security today, I feel, is somewhat mishandled. Indeed, security is neither for the faint of heart nor for the untrained person.**

Can we ever hope to get ahead of the curve?

The way security should ideally be approached is by integrating it within the business processes as, for instance, process plants do with their physical security. You don’t walk into a refinery and define a new business process without keeping very closely in mind that the whole plant might blow up if you aren’t careful. Similarly, no one should design business processes that could jeopardize the integrity of a company’s data. A security expert should be called to attend
all such planning sessions, to ensure security is built into the business processes, and not designed only as an afterthought. We all need to realize that we're under perpetual attack and we need to know how to prevent such situations.

**How many companies spend even a dollar per employee to train them on security issues? To just show them how a link in an email could compromise an entire organization? To teach them not to click unless they know what they're clicking?**

This doesn't seem at all technical, and yet, it is, in my opinion, the single most important area wherein security is lacking, aside from the perimeter defense. Recently, we've taken to calling this ‘the human element’ and finally, our industry has recognized this as the most vulnerable part of any company. And please don't go looking at unskilled employees as the culprits. We're all targets and I personally have witnessed numerous situations whereby a C level employee was the one clicking on a link that was clearly not to be touched.

The difference is that when someone at the lower levels loses their computer, it's quite possible that not much damage will occur. But when a C level does the same, the risk is exponentially higher.

One very common type of attack is aimed at stealing corporate bank credentials; only the CEO and CFO may have those. Once hackers gain that information, they can transfer money to their own accounts anywhere in the world, and the bank is no longer responsible for the loss because the transfer was made with legitimate (albeit stolen) credentials. So, C level people, you above all should take the security class before anyone else in your company! Then embrace security and show to all your employees that it's important, show it by example, show it by creating policies that always include security; just create an environment around you that breathes security (without breathing fear).

Going back to the technical aspects, many tools are available today, to protect your network. A firewall is necessary but please, do not stop there as that was enough way back in 2002. You will need IPS, AV at the gateway, web filtering: you MUST be scanning encrypted streams, and when I say Scan, I mean decrypt, open, scan, re-encrypt – yes a MitM attack of sort – you need to ensure that the company doing this gives you a certificate, which will be used to intercept all the encrypted calls outbound, ensuring that they can be properly decrypted and scanned.

Never connect to your network remotely without a VPN. Never allow anyone who's not a security expert access to your firewall. The common practice of allowing network people to manage the firewall while security people manage the IPS is absolutely to be abhorred; network engineers' objectives are often in contrast with security – they need to get things working and are prone to taking short cuts in order to get there.

A security experts understands the hidden consequences of an incorrect or 'loose' configuration, and will take a few more seconds to think it through, and provide a solution that is secure while still allowing business to continue without interruptions.

**Spend money, where it matters, and do not underestimate the danger, because it is real and it is frightening, my friend. But take heart that it is also possible to contain it. After all, you want to be the one in the parking lot who has an alarm. That way, the thief will move on to the next car – that too is a viable way of doing security.**
Last month, due to the massive increase in the amount of RANSOMWARE on the Internet, Network Box Security Response raised its alert condition to Threat Level 4.

The Internet is under attack. There is serious malicious activity affecting Internet service globally.
Every few hours, there were new variations of delivery mechanisms for these ransomware. Most of it coming via email, using trojan downloaders to download the actual malware over the HTTP/HTTPS protocol, but Network Box Security Response also saw techniques such as advertising network compromise on popular HTTP/HTTPS web sites. (Both the New York Times and BBC websites are well known examples.)

In light of these threats, Network Box advises you to check your gateway security, and ensure that the following best practices are being followed. If they are not, you are kindly advised to follow them now.

1. The majority of this ransomware is coming in as trojan downloaders, or links, in emails. The email attachment contains just a downloader, and the malware itself is downloaded using the HTTP or HTTPS protocols. Accordingly, please ensure that both email and web traffic is scanned.

2. Due to the common use of the SSL encrypted HTTPS protocol for this, and other, malware, please also ensure that you are using HTTPS scanning for your workstations and servers, so as to protect your HTTPS traffic.

3. Network Box recommends that you follow our suggested policy of blocking executable attachments for incoming email.

   (All Network Box systems can do this, either by simple extension block, or by smart content recognition. The ‘.js’ extension (javascript) should, in particular, be blocked as an email attachment. The Network Box 5 platform offers additional heuristics for detection of executable code in email messages, and we recommend all Network Box 5 customers to take advantage of this facility, as part of their default incoming policy.)

4. Often, email messages containing broken malware fragments will be blocked as spam. That is expected, and an effective anti-spam policy, to quarantine spam messages, should be enforced.

5. This is a good time to remind End Users not to open attachments in incoming emails, even if that email says it is from someone they know. Double-check with the sender, if you are not 100% confident.

Be suspicious, be vigilant, keep your data and systems safe.
We are often asked why we can’t just block links to malware. The answer is that while there is a limited amount of malware, the number of links and trojan downloaders is growing exponentially. Quite simply, it is hard to generate a new variant of malware. It is much easier to generate hundreds of thousands of unique links to that one single malware variant.

Most ransomware we see nowadays starts with an email. The email itself will be a short message containing either a link to an external site, or a small piece of script / office macro (the trojan downloader). Both the link and the script/macro operate in the same way - they download the malware executable usually using the HTTP or HTTPS (SSL) protocols.

Network Box offers, and recommends, a multi-layered approach to Internet perimeter security, best exemplified by our response to such malware.

- The original incoming email will be subjected to anti-malware and anti-spam scans. We’ll catch the majority of them in this way, but we can never be 100% successful against such simple links/scripts in spam email. This is the first line of defence.
- The second line of defence is that a policy can be applied to incoming eMail, to block executable attachments. In most business use cases, you can simply block executable attachments, and then whitelist those senders you trust. This is effective against both script and office macro attachments.
- Should the email pass through and be read by a user, education is your third line of defence. Spend time talking to your users about this issue, and make them wary of clicking on links or trusting some random email that comes in.
- Should the user click on the link (or open the office document and enable macros, or execute the script), the network Box HTTP/HTTPS scanning forms the fourth line of defence. Again a full anti-malware scan is performed - but this time against the actual executable itself (not just the link to it).
- For users of the Network Box 5 system, a fifth line of defence is available in policy for HTTP/HTTPS downloads. Just like in emails, you can policy block executable code from being downloaded by your users.

Leveraging all these layers of defence is important to ensure a safe network. Nowadays, it is not sufficient to rely on just one layer.
Contrary to what many Americans seem to believe (FBI and US Gov included), the Harvard report reveals that encryption is no longer just a domestic thing. Though the largest percentage of companies offering encryption software is still based in the US, many other countries have developed their own products. Germany for example, has some very stringent rules pertaining to how private data should be transmitted and stored, and based on these rules, several products have been created, all of which comply with German standard requirements. All these clearly fly in the face of the FBI ‘fuss’ over Apple not wanting to create a backdoor to allowing them to hack iPhones at will. The only people affected by such backdoors would be honest, unassuming citizens. People like you, and like me, who have nothing to hide and therefore, would never go looking for a different encryption. Hackers, criminals and terrorists would, more than likely, acquire someone else’s technology, rendering those backdoors useless, and sending the FBI right back to square 1.

Earlier in 2016, Bruce Schneier of Harvard University - Berkman Center for Internet and Society, collaborator Kathleen Seidel, together with Harvard College student Saranya Vijayakuma, published a report on 865 encryption products from 55 different countries. In the report, Schneier questions the efficacy of any US mandates forcing backdoors for law-enforcement access.
It's especially important to highlight that when you put in a government mandated backdoor, the only ones affected are those who really have nothing to hide. I'm inclined to be not overly bothered by the issue because I really don't care if the FBI checks my texts. There might be other people from whom I want to hide them, but certainly not the FBI because there's absolutely nothing illegal in them!

As such, I may choose to live with any backdoor they put in, in the knowledge that it's unlikely they'll ever need to snoop in my phone. But that backdoor, as the survey authors rightly pointed out, will likely cause vulnerabilities that, if found by hackers, will expose my data to them. And that, I do not want.

Hackers are great researchers; they find vulnerabilities in products before the authors of those products do. Do you think they won't find the backdoors? And when they do, all of Apple's users' data will be exposed. And for what? For the FBI to be able to decrypt the phone of 1 person, who might be smart enough to use a product from another country anyway, thus rendering all this discussion completely moot.

US companies, and US people in particular, need to learn the meaning of “the world is flat”. There's a very nice book by Thomas L. Friedman of that same title which, I firmly believe, both the FBI and the US government should read.

We live in an open world; and the Internet has made it all the more easy for anyone to access anything from their couch. I don’t need to fly to Tanzania to purchase their encryption software; I can just download it over the internet. Geographical barriers are nonexistent, and we all more or less speak English to communicate. So, if I really have something to hide, I’ll just purchase something that isn’t American. Personally, I’m starting to think that even with computing products (routers, switches, laptops and the likes) I need to start looking outside the US.

To be honest, I’m quite tired of this tirade. I’m tired that every time we talk about this topic, the ONLY companies that turn out to be culpable are American companies.

I mean, I've yet to hear of a single Chinese company that has truly been found guilty of such doings; despite all the efforts made by our President to muddy the names of certain Chinese competitors of our major corporations. The Chinese government seems too preoccupied with spying on its own citizens to have time to spy on us.

Besides, what do they really care about the data in my iPhone? Each time we look deeper, the only backdoors we discover turn out to be from US companies.

Are YOU not tired of living in the beacon of the free world, all the while knowing that you're the only one truly being spied upon?

To view the Harvard Report, please use the link below:
https://cyber.law.harvard.edu/publications/2016/encryption_survey/
The Network Box Notification System gives users very fine control over the notifications they receive. Notification types (e.g., service ticket updates, GMS tickets creation, etc.), can be customized to be delivered to different contact points (such as ‘office email’, ‘out-of-office email’, ‘mobile phone’, etc.) and the time frames they want those contact points to be active (e.g., Monday-to-Friday 9am to 6pm - send ‘service ticket update’ to ‘office email’).

The system supports multiple contact types for Mail, SMS, Mail-To-SMS gateways, iOS/Android PUSH, as well as several IM services. An ‘audit’ contact type is also used to record a history of notifications.

Notification Methods

Notification methods are mechanisms used to deliver notifications to end users. By default, the Network Box Notification System, is set to email-type notification, however, users can (and should) extend this default behavior. Consider the following typical scenario:

What is the arrangement if your Network Box or mail server becomes unreachable and there is a problem outside office hours?

- By creating an out-of-office notification email address (for example, with a Gmail or other such external email addresses), you can continue to receive notifications even if your internal mail system is not reachable/functioning.
- If you have a mobile iOS/Android device, installing and logging-in to the Network Box App will create a Notification helper that will use Apple and Google’s notification/messaging service to deliver alerts to you.
- Network Box also offers the SMS notification method, for delivering SMS alerts directly to your phone.
Time Based Control

Each notification contact point you create can have filters attached to restrict notifications to limited time ranges. For example, you probably want your out-of-office notification contact point to only be active out-of-office-hours (which you can do by configuring notifications to only be sent Monday to Friday 09:00–18:00).

NOTE: In your Box Office My Account page, there is a Time Zone setting. This defaults to UTC (Coordinated Universal Time), but you can set it to the closest time zone to you, and the rest of Box Office will change to show dates/times in your desired time zone (even if the box or SOC is in a different time zone).

Notification Configuration

The Network Box Notification System offers a sophisticated facility to notify users of changes and events they need to know about. This is configured using My Account (and the Users Module) within Box Office. Configuration is performed in two stages:

First, you create Contact Types (which are methods you can be contacted at, and filters to define when these contact types should be used). Then, you update the Notification Config to let the system know which events you want to be notified on, and which contact types to use.

❖ Creating a new Contact Type

Let's start by creating a Contact Type by clicking Add Contact Type in My Accounts > My Account Information > Contact Types:

You will be taken to the Add Contact Type page. Here, you will need to give the contact type a name (a friendly name that you can choose), and choose the method to be contacted by. You can choose from Audit, Email, SMS, or Mail-To-SMS. When you have finished, click the Add button.
For the following Contact Type, you may be asked to enter additional information, as follows:

**Audit** is used to create an audit trail of notifications. It does not send out any notifications, but merely records a notifiable event in your notification list (shown under Overview / Notifications).

**Email** is used to notify you by SMTP eMail. You can choose an email template to use, and enter your email address that you want to receive the notifications on.

**Mail-To-SMS** is used to notify you by Mail-To-SMS gateways. Your Mobile Phone Provider may provide such a service, whereby Network Box can send an email to your Mobile Phone Provider gateway, and they forward it on to you as an SMS. You can choose from the list of supported gateways, and enter your Mobile Phone number in the provided field.

**NOTE:** this is only offered for a limited number of Mobile Phone Providers, and the provider may charge you for this service. If you are using a provider not listed, and you are certain that the provider offers such a service, please let your regional SOC know the details and we will arrange to add support.

In addition, with each contact type, you can either enable or disable the contact (using the Enable check box) to start / stop notifications, and you can choose whether you want to be notified for all events (including those initiated by yourself), or only those initiated by other people, using the Notify Myself check box.

You can also define the periods that you want to be notified:

The default (if you don’t specify anything) will be to notify you at any time of the day, any day of the week, but you can Add notification periods to the Contact Type, to choose the day of the week, time of day, and boxes that you want this Contact Type to be restricted to. The Boxes lists come from the Boxes module, where you define them as search Queries.

Once you have defined a Contact Type, you should click the Test button to test it and ensure you receive a notification correctly. **NOTE:** the test facility is not filtered by Notify Period, and should always get through to you.

---

**SMS** is used to notify you by SMS message to your mobile phone. You should enter the mobile phone number that you wish to be notified using.

**NOTE:** your Mobile Phone Provider may charge you for SMS messages received using this facility. To use this facility you must also obtain SMS credits from Network Box. Each SMS credit can be used for one SMS notification. Once your credit balance reaches 5, an extra (free) warning SMS will be sent to you, to let you know you need to top-up your SMS balance. Once your credit balance reaches 0, an extra (free) warning SMS will be sent to you, to let you know that you will not be receiving any further SMS notifications until your balance is topped up.

**A Mobile App V5 Contact Type** can be created from any supported iOS/Android device running the Network Box App. Just answer ‘OK’ when the App asks you if you would like to receive PUSH notifications, and the Contact Type will be created for you automatically (and tied to the connected mobile device).
Notification Config

Once you’ve defined your Contact Types, you should define the Notification Config. To configure this, click **Edit** in:

*My Accounts > My Account Information > Network Config:*

You will be taken to the Network Config page. It is recommended that you define the Notification Config as below:

For each notification type and Contact Type, you can choose if you want to receive that notification. The notification types are:

- **Service Ticket creation**, update and reminder (for service tickets)
- **GMS Ticket creation**, update and reminder (for Global Monitoring System health tickets)

Each notification type is further broken down into:

- **All**
- **Waiting for Customer**
- **Waiting for NOC**
- **My Tickets**

These are used to indicate the state of the ticket (matching All tickets, only those waiting for you, only those waiting for the SOC, and only tickets you created, respectively).

*With fully comprehensive and customizable options, the Network Box Notification Systems offers users very granular control over their notifications, and helps to streamline the communication between the SOC and the end user.*
Network Box

Mobile App for iOS and Android platforms

Network Box is pleased to announce the release of the new mobile App for iOS and, for the first time, Android platforms. The Apps are available, as free download, on the Apple iTunes App store and Google Play store. You can find them with a search for Network Box in the business category.

This version of App is fully integrated with the Network Box Notifications System and adds support for the iOS APNS (Apple Push Notification Service), and Google GCM (Google Cloud Messaging). By augmenting the Network Box Notification System, finer control of notifications can be applied by the user:

‣ Set-up notification schedules
‣ Configure the type of notifications
‣ Group boxes and notifications

In the App, there is a Notifications tab, to allow you to see notification history.

When you run the App for the first time, it will ask you for permission to send you notifications. If you answer OK, it will automatically create a Mobile App V5 Notification Contact Type, tied to your mobile device, for you to manage the notifications.
At the heart of the Network Box 5 mail scanner is a pattern engine. It takes signatures (lists of patterns) and applies them to the different component parts of email messages, in order to classify email content as spam, phishing, malware, pornographic, etc. There are many different sorts of signatures present in the mail scanning signature sets, but by far the most common are pattern matching rules.

Rules that say things like ‘look for a part of the message that contains words starting with advert’, or ‘find the letter p, followed by a small number of optional symbols, followed by the letter e, etc’. For a typical email, out of perhaps 250,000 signatures, 10,000 to 20,000 such patterns would be run during the classification phase. A simple string search would be fast and efficient, but not powerful enough for effective content classifications; so it is this powerful pattern matching engine that permits complex and accurate classification in Network Box 5.

We are proud to say that after 8 months of development and testing, we are now ready to release the latest pattern engine for the Network Box 5 mail scanning system. The primary goals of this new engine were to improve performance and accuracy.
To achieve these, we’ve implemented the following changes:

1. There are several hundred thousands patterns in the signature set - corresponding to known aspects of current email seen on the Internet. Running all those patterns over every single component part of the email is not required, as certain pattern checks are only required for certain types of email component. So, the new Network Box 5 mail scanning rules engine allows for specific sets of patterns to be run for specific types of email component - dramatically reducing the total number of pattern checks that we need to perform.

2. We’ve now got a facility whereby the matching of one particular rule can now enable another set of rules to be run. For example, certain trigger patterns can be used to enable an extended set of rules for further in-depth scanning.

3. The core pattern matching engine itself has been replaced with one optimized for the task at hand. Previously we used a standard backtracking regex engine, but our new replacement is based on an optimized finite-state machine using automata theory. Our new engine provides very predictable memory and CPU resource utilization, with a typically linear relationship between size of object to be scanned and scan time. This replaces the previous backtracking regex engine we used, which suffered from exponential CPU usage as the size of the object to be scanned increased.

4. The signature set we use has also been optimized, based on feedback from real world spam campaigns we are currently seeing.

The overall performance improvement of the new engine is hard to quantify, because it depends on the size and composition of emails to be scanned. But, in general, we are seeing a two to three times performance improvement, and corresponding reduction in email scanning times, with the new engine when compared to the old.

This new mail scanning pattern engine is being released to all Network Box 5 customers, in the July 2016 patch tuesday.

Network Box 5
Mail Scanning ‘bulk’ Classification

A large proportion of the submissions to spam@network-box.com or from our spam traps, are newsletters. Messages sent to a large number of people, who may or may not have subscribed to the newsletter perhaps years previously. The problem is that we have no way of knowing whether the recipient subscribed himself, was subscribed by someone else, or merely added to the list by unscrupulous senders. A large number of bulk email delivery services and users seem to subscribe to the notion of it being easier to beg for forgiveness rather than ask for permission. Opt out, rather than opt in.

We cannot simply mark such newsletters as spam, as the emails are required by many of our customers.

We cannot simply blacklist the bulk email delivery services, as many are used by legitimate senders as well as unscrupulous ones.

So, in the July 2016 patch tuesday, we have introduced a new email classification ‘bulk’. When we detect an email which appears to be going to multiple recipients, as part of a mailing list, newsletter, or such bulk distribution service, we will classify it as ‘bulk’. Customers can now use this to be aggressive against such bulk email, or to control it by whitelisting.
In August 2016, Network Box released support for a new URL category “INFL botnet cac”, in Network Box 5. URLs categorized as this are malicious in nature and used by botnet clients to access botnet command and control servers. As such, we recommend such accesses be denied, and include this category in both our standard nb-core and nb-malware ACLs.

**Category:** INFL botnet cac  
**Title:** Infected LAN botnet command and control

This category includes URLs which have been classified as malicious and part of known botnet command and control networks and protocols. Typically, botnet clients use these URLs to communicate with their command and control servers. The category is very precise and there is a low risk of false positive.

The **Proxy Infected LAN** security module subscribes to a PUSH update signature set of several thousand malicious URLs used by known botnet command and control centres. This URL categorization support extends the botnet IP address support provided by the base “Network Infected LAN” security module. We currently provide URL categorization coverage for:
- cryptowall
- feodo
- locky
- palevo
- teslacrypt
- torlock
- zeus
- and other common botnets.

Customers using the Proxy Infected LAN and web client content filtering security modules can now take advantage of this new category by either blocking the nb-core and/or nb-malware category ACLs, or specifically blocking category “INFL botnet cac”, in their web client policies.
At the time of writing this article, attacks against web servers are (by far) the most prevalent issue in cyber security. A Data Breach Investigations report for 2014 showed that 35% of breaches were caused by web application attacks. And by mid 2016, this number is only rising.

Hackers are getting control of web servers for different reasons, the main ones being the ability to control a server and spread malware. Often, these two objectives go hand in hand.

**Why do hackers want to control a web server?** Because a server is often hundreds of times more powerful than a workstation, and that allows them to have a platform to launch attacks from a single point, rather than having to deal with multiple workstations. Servers are often also connected to larger bandwidths, enabling these attacks to be increasingly efficient. They are also online 24/7, users don’t turn them off at night as they tend to do with a personal computer. And they are connected to public IP addresses on a public network, not in someone’s home or office. A server can, and most times is, used as a command and control center to manage a network of zombies – a botnet. Finally, a server can be used to ‘serve’ malware. In this case, the web server may not even look compromised, and yet malware lurks in the background, ready to attack unaware browsers.

---

**Why you need WAF**

by Pierluigi Stella  
Chief Technology Officer  
Network Box USA

---

21
This should make one thing abundantly clear – protecting web servers is critical; not only does a company stand to lose data, the server can also be used as a bridge into the company’s network. Or to launch attacks against other companies; and although we have yet to see lawsuits in such cases, it is only a matter of time before someone gets sued over allowing their server to become a tool for conducting attacks against someone else.

But how exactly does one protect a web server? Especially one that is running an application, which is, in turn, connected to a database?

Up until a few years ago, the practice was to put the web server itself into a DMZ, the database server on the LAN, and ‘hope’ that the firewall and IPS could stop malicious traffic between the two. The idea being that if the web server were to become compromised, it is easy to rebuild and data is not lost. Unfortunately, this method of protection is insufficient; it never really was to begin with, but today, it is clear how and why.

First of all, too many people misinterpret the meaning of DMZ and allow all traffic, rendering the very idea of DMZ pointless. Second, the ports needed for the web server to run queries against the database are the very ports hackers are trying to attack. This does not in any way prevent a SQL injection or a database DDoS attack, as both methods use database ports that are open from DMZ to LAN to allow the web server to run queries.

The next idea was to set up IPS in line with firewall, to intercept malicious traffic. Though not a bad idea, it is, unfortunately, very limiting. An IPS is a layer 3 protection. Think of it as an AV at the packet layer. It reads the content of a single packet in a stream, inspects it against known vulnerabilities and exploits, using a mix of signatures and heuristics (behavior analysis). And that is all it does. You might be wondering what the issue is. IPS is used for many different reasons. The problem is that IPS is a layer 3 protection, whereas HTTP is a layer 7 – it is an application layer protocol. And web servers run applications. This means that attacks can be carried on using transactions that span across several packets or streams; and each packet or stream can appear to be perfectly clean. An IPS can protect against some low level SQL injections and XSS attacks; it can protect against things like the Slammer worm, on which more information can be found here:

https://en.wikipedia.org/wiki/SQL_Slammer

SQL Slammer is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It spread rapidly, infecting most of its 75,000 victims within ten minutes. The reason why that is possible is because the Slammer was less than 400 bytes in size, so the entire malware fit into one single packet.

But a web server attack of recent times is almost never just a single packet of malware. More often than not, such attacks try to work around the HTTP protocol, injecting commands that are not part of a normal sequence, to gain access to resources on the server or cause the application to react in a way it wasn’t designed for. In other words, an IPS cannot understand web application protocol logic, and cannot fully distinguish if a request is normal or malformed at the application layer.

In part two of this article, we will explain (at length) why an IPS is ineffective when it comes to providing a safeguard against application vulnerabilities.
In the last article, we touched on the critical value of protecting one’s web server, and the various way to do just that such as the setting up of a DMZ or the creation of an IPS. We also introduced the fact that while a good idea, establishing an IPS in line with firewall as a means to intercept malicious traffic, was limiting. Continuing from that, we will focus on the specific role of WAF and what this really means to your webserver.
As explained previously, an IPS cannot be effective against all potential application vulnerabilities. Typically, an IPS ends up producing too many false positives, which in turn yield two possible reactions – either:

1. it delays application response time and incorrectly interferes with the application; or
2. it allows attacks as normal behavior in an attempt to reduce false positives.

An IPS looks at signatures and anomalies; a WAF looks at behavior and logic, analyzes traffic in both directions, looks at what is being requested, and what is being returned.

A Web Application Firewall’s main task is to protect web applications by inspecting the semantics of the flowing traffic and also inspecting HTTP/HTTPS for typical attacks at layer 7 such as:

- SQL Injections
- Buffer Overflow
- Cross Site Scripting (XSS)
- File Inclusion
- Cookie Poisoning
- Schema Poisoning
- Defacements
- and many more...

To obtain a better understanding of the topic, a good source of information is found at this link:


OWASP is an open software security community collecting, among other things, the list of top attacks against web servers. Any WAF on the market today will have to at least protect web applications and servers from the OWASP top 10.

Another aspect of using a WAF is called SSL offloading. The internet is headed towards complete encryption. Increasingly, websites are using HTTPS, even when there is no confidential data to be protected. If the website runs an application that requires confidential data to be entered, such as your online banking portal, the choice of HTTPS is obvious. But there are plenty of examples of sites that are using HTTPS even though in principal they wouldn’t need to, because there is no private data to be protected.

Soon after the NSA scandal of 2014, Google.com chose to use HTTPS for all their pages. Yahoo! has done the same. And the examples are countless. Encryption is adopted not just to hide searches, but to also guarantee the authenticity of a website. Too many attacks are conducted by spoofing the looks of other websites, and the mechanism of private/public key/cert inherent to the HTTPS protocol is likely the last bastion against a widespread diffusion of such attacks.

For instance, when you go to https://www.network-box.com/, the certificate on that website (published and guaranteed by a certificate authority) tells your browser that you have indeed reached the intended site, and not some hacked, spoofed site that might try to collect information to, in turn, conduct an attack against you.
What does this really mean for one’s webserver?

If the server capacity was designed for HTTP and suddenly every single transaction is encrypted, the CPU load can become such that the server itself may not be able to handle it. One feature where a WAF can help is HTTPS offloading – the certificates are placed on the WAF, the encrypted connection is terminated on the WAF. Between this and your servers, the traffic does not necessarily need to be encrypted, thus “offloading” the function to the WAF. This allows control over which version of TLS to use. That said, given that every version of SSL has now been compromised, so in reality, no one should really be using that for their HTTPS protocol. Yet we still see many websites that have not been updated and corrected, likely because the software version cannot be updated (for the reasons explained earlier). The WAF can easily enforce the use of the appropriate TLS version, without the need to touch anything at all on the web server.

Because the WAF decouples the traffic between web server and internet, and the browsers are no longer connecting directly to the webserver, a WAF is an inbound proxy. Once we consider this, we see how it is possible to deploy other technologies commonly applied to outbound proxies to a WAF, such as AV and access control. Applying AV rules to an inbound proxy may sound like a stretch because of possible performance limitations, and there are certainly issues with this; but it is vital to remember that in this case, we are not protecting a workstation.

We are protecting a very specific technology; so the applied AV can be limited to only signatures and heuristics that are relevant to a web server; there is really no need to run 11 million signatures to protect a web server. And this can make running an AV more plausible.

At this juncture, it is also worth mentioning what WAFs do not do.

A WAF will not enforce access control in the traditional meaning of the term. Do not be confused by the term “firewall” present in the name of this technology. A WAF only protects the server farm behind it, adopting signature based or anomaly detection algorithms but, unlike a network IPS, it will focus only on the HTTP and HTTPS protocols. A WAF is a layer 7 technology, not layer 3.

Some Web Application Firewalls will also provide layer 7 protection against DDoS attacks, although most vendors separate the 2 types of protection, offering specific DDoS protection as a different service or appliance. However, since this article pertains to WAF, we will not dwell on the details of DDoS attacks against web servers and why protection against such attacks is equally necessary.

Gartner’s magic quadrant for WAFs says:

- Protect web applications against hackers’ attacks, to monitor access to the web applications, and to collect access logs for compliance/auditing and analytics
- Primary WAF benefit: providing protection for custom web applications that would otherwise go unprotected by other technologies that guard only against known exploits and prevent vulnerabilities in off-the-shelf web application software
- WAF technology
  - Maximizes the detection and catch rate for known and unknown threats
  - Minimizes false alerts (false positives) and adapts to continually evolving web applications
  - Ensures broader adoption through ease of use and minimal performance impact

There is another aspect to WAF technology that must not be underestimated. A web server runs 2 ‘applications’ – the web server itself (be it Apache or IIS or something else) and the user application (what you see when you go to that website). And in between, there are the tools used to develop the user application itself. These could be PHP, Wordpress templates, Java, ASP, you name it.

Each of these layers can have vulnerabilities. Apache has its own and plenty of them; IIS does as well. But these are often known, announced, patched and therefore, made irrelevant after a while. Aside from that, once they are known, it is often possible to create IPS signatures that can protect the web server itself.

The real issues, the ones that can cost an organization its entire database, are those caused by the user level application and tools used to develop it. Whether it is an off-the-shelf product or one developed in-house (which is most often the case), software invariably has errors, which leads to vulnerabilities. It is not a matter of if, but how many, and how exploitable.

For example, PHP and Java have vulnerabilities. But these aren’t tools you can always update as this (act) could break the actual application. As such, these tools are often not updated, vulnerabilities are not patched, and they cause the application to be, well, laid bare and open to attacks.

In our third and final article on Why you need WAF, we will discuss the inherent security pitfalls in the applications we use.
Over the past two articles, we outlined how vital it is to provide a robust security posture for one’s web server and the various options currently available. In today’s concluding installment, we take a long, hard look at web applications.
For instance, what web application you’re currently using? More than likely, it was not developed with security in mind. No matter how much we discuss the topic and we talk about security driven web application development, how many people and companies really even know how to do that? How many developers test their web applications from a security stand point?

And what if the web application in question is old, a legacy development that was written 10 years ago? Developers have moved on, documentation is scarce, if present at all, and yet the web application plays a vital in your company’s business.

Updating the tools it relies upon isn’t even a question – the application will break. Fixing the web applications issues may well be even harder and often unfeasible. The entire construct is a vulnerability disaster waiting to happen. This is likely the most important example of where a WAF can be very useful.

A WAF will have a configurable layer where a business owner, or vendor can create specific signatures. Therefore, instead of breaking the web application, or living with one that is vulnerable and can expose confidential data, a WAF allows for the creation of customized protection, if you like, dedicated signatures tailored to very specific web applications. This allows organizations to achieve strong protection for their web applications without the need to alter functionalities, and without having to fuss over updating them in a rush.

Note that we are not advocating running that old COBOL application for the next 40 years. And yes, sooner rather than later, we’d be better off scraping everything and rewriting applications with more advanced tools. But the adoption of a WAF ensures that process to be just that – a process – instead of a frenzied decision dictated by the need to cover up security holes.

We hope that you’ve found these articles on why you need a Web Application Firewall (or WAF) informative and useful. Today’s threat landscape being this dynamic and fast-paced, organizations that fail to adequately arm themselves do so at great (financial and operational) risk.
Network Box has always pioneered the use of the PUSH, as opposed to PULL, method of signature distribution. It is quite simply the better way of doing the job.
Most other security vendors configure their devices to poll (PULL) for updates once an hour or so, while Network Box SOCs deliver updated signatures in real time as soon as we get them, and within 45 seconds globally. Then, once we've downloaded the signature updates, we install them, and check that they are working and up-to-date; all automatically and in real time.

With the Network Box 5 platform, we've improved our PUSH update technology even further by introducing record-based, in addition to file-based, updates for incredibly granular delivery of new protection signatures.

However, there are times when even this is not fast enough - especially for cases where the size of the signature database is massive and cloud based. For that, we have the Network Box 5 reputation services which offer online real-time lookup of the reputation of file hashes, IP addresses, email addresses, URLs, etc. This month, we're proud to announce the release of three new reputation services for Network Box 5 customers:

1. **NBL** - The Network Box IP address reputation service
2. **EBL** - The Network Box email address reputation service
3. **UBL** - The Network Box URL reputation service

Each of those databases is updated in real-time from the Network Box Security Response OUTBREAK system - tracking the status of millions of threat metrics from both our own as well as partner systems. Each system provides reputation confidence scores for malware, spam and policy classifications. The reputation scores themselves are distributed to the Network Box Cloud DNS system; typically once every 3 seconds. Network Box 5 boxes access these reputation scores over the public DNS system, in real-time.

It is our Security Response Team and the Managed Services we provide that continue to differentiate Network Box from other security providers. Not relying on just PUSHing the latest threat protection signatures to managed devices, we continue to expand on our online reputation services where appropriate.

**ADMIN and USER web portal access via names**

The admin and user web portals are typically accessed via the IP address of the box, using the ports 4242 & 4244 (for HTTP), and 4243 & 4245 (for HTTPS), respectively.

With the November 2016 release of Network Box 5 firmware, we are also now offering an optional automatic re-direct to allow access to the web portals, for users behind Network Box protection, using the DNS names admin.network-box.com and user.network-box.com. The access URLs offered are now:

**Admin Web Portal**
- http://admin.network-box.com/
- https://admin.network-box.com/ (for TLS/SSL secure access)

**User Web Portal**
- http://user.network-box.com/
- https://user.network-box.com/ (for TLS/SSL secure access)

This is in addition to the existing kiosk.network-box.com (for Captive Portal kiosk mode authentication).
As 2016 closes, it seems a good time to look back and see what has changed in the security landscape, as well as try to anticipate what we have to look forward to in 2017 and beyond.

One thing that has become abundantly clear is that the front lines of Internet Security are becoming more complex. Up until recently, we put our servers in a DMZ, workstations in a LAN, and did all that we could to defend them on a single front of perimeter security – with attacks primarily coming from the Internet. Nowadays, however, all that is changing; servers are in the cloud and our users are on mobile devices out on the streets. Now we’re fighting the battle on at least three fronts. Ask anyone with military experience and they will tell you that is not a good position to be in; you have to defend all those places, while the attackers have to just find one area of weakness.

The old days of brute force attacks and network vulnerabilities are thankfully mostly behind us. We’ve learned to patch regularly, and the Internet has helped us easily obtain and install those patches (often in an automated manner). But we now have a huge number of Internet Connected Devices – from light bulbs to door locks – and those devices are often riddled with vulnerabilities, have back doors, and are not so easy to apply security patches to.
The attacks are also growing in sophistication. The old days of blatantly obvious phishing emails have gone, and we are now faced with perfectly phrased persuasive messages that confuse even experts as to their authenticity. One click, and a stream of exploits are downloaded to install ransomware that can then spread over the local network behind firewall protection. If an expert cannot easily tell whether these are fake or real, how can a junior office staff be expected to know?

And above all else, the attacks are growing in speed. I am reminded of that line in Top Gun when Commander Stinger is told the aircraft launch catapults are broken and will take 10 minutes to fix; his reply of ‘Bullshit ten minutes! This thing will be over in two!’ reflects the problem facing the network security industry nowadays. We’re used to and comfortable with the technology of signature protection – but even drastically reducing the time to producing and releasing those signatures from hours to minutes will make little difference to an attack that runs to completion in two minutes. Take any zero-day malware and upload to virustotal.com; it is common that none of the 50+ mass-market anti-malware engines have protection for at least the first hour of the attack. The malware writers simply test their creations are undetected, prior to release to millions of targets within seconds, via huge botnets of compromised hosts.

As for 2017 and beyond?
...more of the same.

Sure, we can increase the speed of our signature release (Network Box pioneered the move from pull to push signatures – decreasing release times from days/hours to 45 seconds or less). We can remove the need for signature release entirely by leaving the signatures in the cloud and doing real-time lookups (Network Box addresses this with our Z-Scan engines) and that brings the protection deployment time from first sample down to 2 or 3 seconds. We can even remove the need for signatures altogether by heuristic / emulation technology (Network Box has several heuristic / emulation engines in our Network Box 5 product today). But, even with all that, we are not addressing the core fundamental problem that to succeed, we need to defend against 100% of attacks successfully, while to fail the attacker only needs to get through ONCE.

Network Box has been preaching for years now that the solution to these new threats to the security landscape is a change from signature based to policy based protection. The Network Box 5 system is at its heart, a classification and policy engine. We look at streams of network data (email messages, web downloads, etc) and classify them (spam, ham, malware, executable, dlp, etc). Policy is then applied to permit/deny the transfer, and it is the effectiveness of that policy that is the key to the security of the assets it is protecting.

The Network Box anti-spam and anti-malware engines do an incredible job at detecting such malicious data streams, and use dozens of protection technologies including heuristics, emulation, zero-day cloud based signatures, reputation lookup, as well as signature protection delivered by push updates. We even offer SSL interception and decryption options to be able to do this within encrypted streams.

Despite the changing security landscape, our recommendation today remains the same as it was ten years ago:

- Customers should move from relying solely on blacklist based policies (where everything is allowed through except for that scanned to be malware / undesirable), to a whitelist based policy (where executable and otherwise suspicious content is denied, except from those specifically whitelisted senders).
- At the firewall level, we’ve moved from ‘allow all, but block tcp/22’ to ‘deny all, but allow tcp/80’. Most have now also moved to similar whitelisted based policies outbound.
- But, at the stream level, we are still allowing executable content into our network. We need to move to a policy where executable content is blocked (blacklisted), except from specific trusted senders (whitelisted).

It is the role of Network Box Security Operation Centers to help you enforce that policy.