HAKIN9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

NETWORK SECURITY

BUILDING AN EFFECTIVE SECURITY STRATEGY

KEEPING YOUR ENTERPRISE'S NETWORK SECURE

ENHANCING YOUR NETWORK SECURITY TOOLS

Vol.7 No.09
Issue 09/2012(57) ISSN: 1733-7186

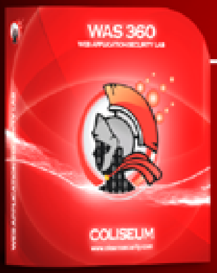
PLUS

AN INTERVIEW WITH ALEX KIRK FROM SOURCEFIRE

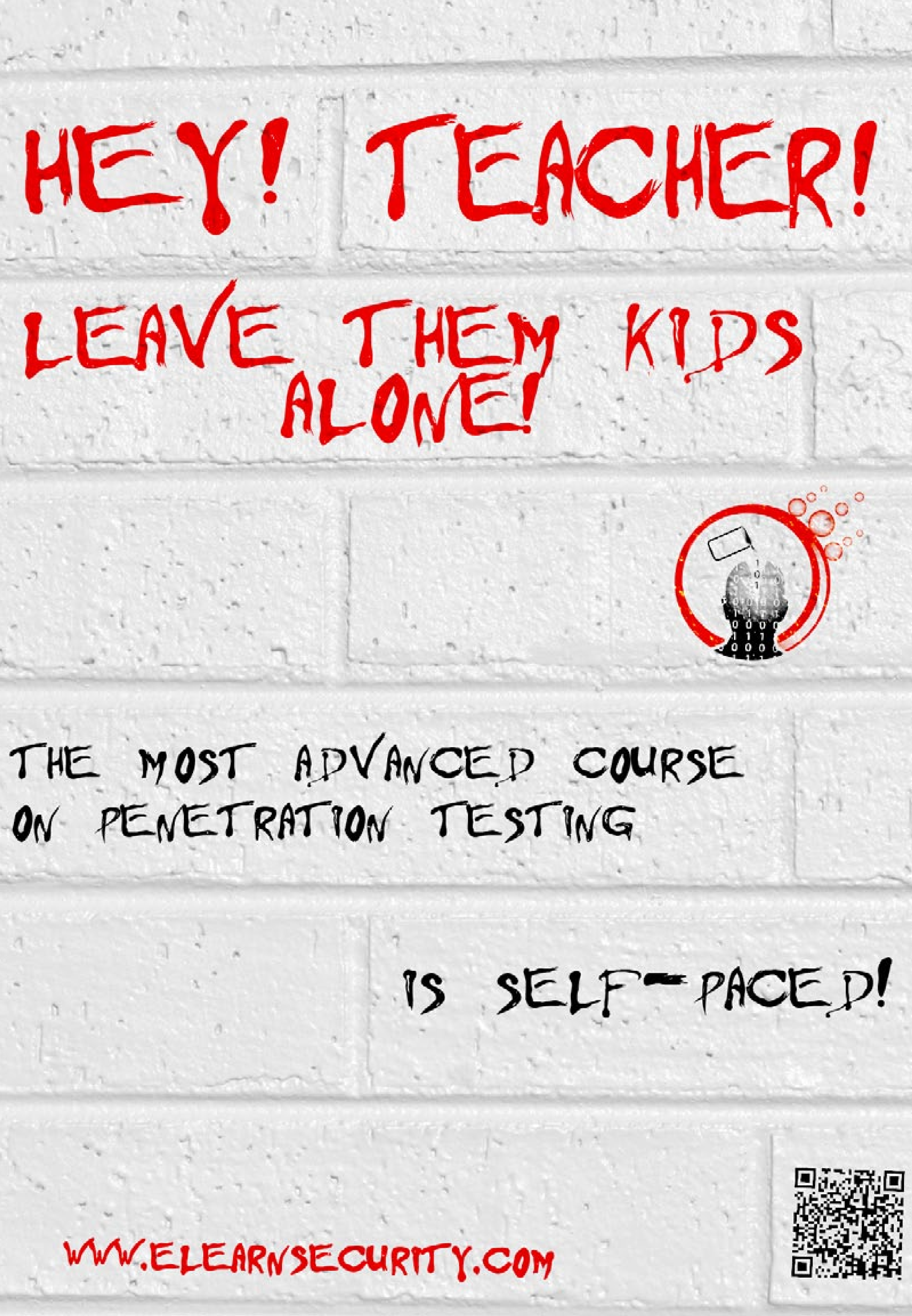
RIFEC REVIEW OF FORESCOUT TECHNOLOGY

Module 5: Post Exploitation
Network Security

The following summarizes the idle scan steps:


WAS 360
WEB APPLICATION SECURITY LAB
COLISEUM

HERA
VIRTUAL LAB
HERA


HEY! TEACHER!
LEAVE THEM KIDS ALONE!
THE MOST ADVANCED COURSE ON PENETRATION TESTING
IS SELF-PACED!
WWW.ELEARNSECURITY.COM

Hakin9 team

Editor in Chief: Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Managing Editor: Ewelina Sołtysiak
ewelina.soltysiak@hakin9.org

Editorial Advisory Board: *Rebecca Wynn, Matt Jonkman, Donald Iverson, Michael Munt, Gary S. Milefsky, Julian Evans, Aby Rao*

Proofreaders: Jonathan Edwards, Steven Atcheson, Ewelina Soltysiak

Top Betatesters: Amit Chugh, Gregory Chrystanthou, Griff Reid, Aidan Carty, Rod MacPherson

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

To create graphs and diagrams we used smartdraw.com program by SmartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Hakin9 followers,

This month's issue is devoted to network security. We have many articles that were written especially for you by network security experts. The first article is by Pauli Laine, who will discuss the challenges of traditional security and will show how these challenges can be faced with the Next-Generation Firewall, which, in turn, will lead to the alignment of IT operations with contemporary business needs.

We also have an article by David Berdeaux, who shares his proposed security enhancements to the 802.11 Protocol and wireless routers. Mads Becker Jørgensen will discuss his approach to creating a security strategy, while Alex Martin will talk about Unified Threat Management technique in order to show how to save time and money without losing security. Claude Labbe on Netflow, will discuss how to use Netflow and its information to track network events. We also have an article for you written by Chris Weber who will discuss the Cisco PIX 500 Series Security Appliance.

We will also feature a review of ForeScout Technology's Mobile Security Software by Sembiante Massimiliano and an interview with Alex Kirk from SourceFire.

Hakin9's editorial team would like to give special thanks to the authors, betatesters, proofreaders and our editor in chief, Grzegorz Tabaka.

I hope that you will enjoy reading this issue!

Ewelina & the Hakin9 Team.

NETWORK SECURITY TOOLS

NETWORK DESIGN

ENTERPRISE SECURITY

EXTRA ARTICLE

Disstrack

A new series of malware is out which takes a new stance on the machines it infects – it destroys them. This malware specifically targets computers in the Middle East. Once Disstrack gets ahold of its victim machine, it renders the hard drive inoperable. As part of the Shamoon attacks, Disstrack is comprised of several components: dropper, wiper and reporter. According to Symantec, the dropper is the main point of infection and "drops" several other modules onto the system. The wiper is responsible for the destruction and the reporter connects back to the attacker. After the malware has deployed itself, it destroys files and overwrites the master boot record (MBR). The main attack vector used to spread the virus across the internet is unknown but once it is on a server, it copies itself to other network shares. More detailed information can be found on Symantec's site: *http://www.symantec.com/connect/blogs/shamoon-attacks*

by eLearnSecurity

At&t

The communications company was victim to a distributed denial of service attack against its DNS servers. The attack disrupted the service of many At&t business customers but the attacks were quickly mitigated. Their official statement said:

"Due to a distributed denial of service attack attempting to flood our Domain Name System servers in two locations, some AT&T business customers experienced intermittent disruptions in service on Wednesday. Our network and security teams quickly worked to mitigate the impact and service is currently running normally. We apologize for any inconvenience to our customers".

At&t does offer, as an additional service, advanced DOS protection for its customers. Details on whether or not this had any impact on that attack have yet to be released.

by eLearnSecurity

SMS Zombie

Another strain of malware has running rampant across Android systems, mainly in China. TrustGo discovered the malware and states it may have infected 500,000 mobile devices by now. The malware stays mainly in China as it exploits a vulnerability in the China Mobile system. The app continues to spread through online forums and infected apps in the GFan marketplace. The malware is installed as a wallpaper. Once the user sets it as the wallpaper, it prompts the user to install additional files/modules. Once those are installed, the malware payload has been delivered to the device. The malware has control over certain parts of the device but its main purpose appears to monitor the SMS of the phone. If it sees specific (defined) keywords, it forwards the message to the command and control servers.

by eLearnSecurity

AMD Forum

Advanced Micro Devices had to shut down their forum on August nineteenth after the hacker group, r00tbeer, defaced it and claimed to have stolen a database of information on AMD staff. R00tbeer announced the success of the attack on Twitter shortly after and included a link to Twitter in the forum defacement. AMD immediately shut down their site with a message claiming they were taking down the service for maintenance. Many reports state that AMD used the WordPress blogging software for their forum. Paul Ducklin of the Sophos Naked Security site detailed the attack, reporting that 189 usernames and PHP-Pass passwords were leaked. He states "All in all, a small deal in the history of security breaches. More of a hackette than a hack, and no AMD customers need to panic, which is good news. But every hack is, at its heart, bad news. If only we were collectively more conscientious about patching against criminals, and if only those criminals were more likely to be caught!"

by eLearnSecurity

ELEARNSECURITY

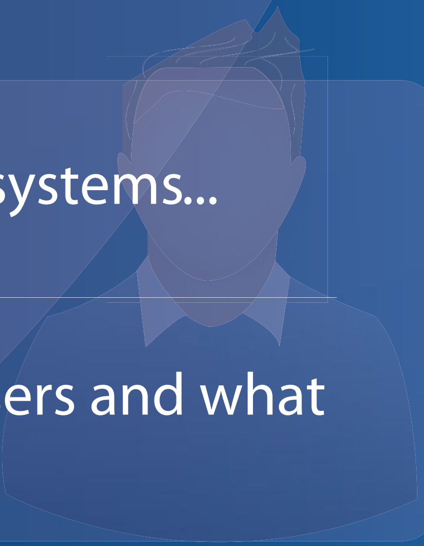
Based in Pisa, Italy, eLearnSecurity is a leading provider of IT security and penetration testing courses for IT professionals. eLearnSecurity's mission is to advance the career of IT security professionals by providing affordable and comprehensive education. All eLearnSecurity courses utilize engaging eLearning and the most effective mix of theory, practice and methodology in IT security – all with real-world lessons that students can immediately apply to build relevant skills and keep their organization's data and systems safe. eLearnSecurity provides the ECPPT (eLearnSecurity Certified Professional Penetration Tester) a certification that is trusted by companies worldwide. eLearnSecurity's practical approach promotes certifications that prove a students' ability at performing real world tasks.

idtheft
protect

Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...

Be proactive...



- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...

ID Theft Protect provides information on threats from a user perspective.

Visit: **http://id-theftprotect.com**

Real-Life Experiences

with Next – Generation Firewall

The traditional way of doing network administration and network security has been promoted for over ten years. It was started even before business strategy and IT strategy was built or even aligned with IT operations. It has evolved since the 2000s, but is the trend supporting business needs?

What you will learn…

- The challenges of traditional security
- How to face these challenges with Next Generation Firewall
- Real life environments with next generation firewall solutions that will align business requirements with IT operations

What you should know…

- What a typical network consists of – balancers, firewalls, VPN gateways, proxies, LAN, WLAN
- SSL encyrption/decryption
- Unified Threat Management (UTM) definition

This article describes real-life environments with next-generation firewall solutions designed in order to align business requirements more efficiently with IT operations. It points out common challenges and how to deal with constantly demanding business requirements faced by the IT operations in the administration point of view.

The traditional way of doing security

A typical corporate network consists of load balancers, firewalls, VPN gateways, proxies, IDS/IPS, switches, routers, antivirus, anti-spam systems, LAN, WLAN and WAN. Since the network consists of so many systems, there is a need for centralized logging system and perhaps for a *Security Information and Event Management* (SIEM) solution for managing and analyzing the huge amount of log information and to get rid of the "background noise" that unnecessary events generates. Since we must manage all the network devices, we need to have centralized management systems whenever possible and reasonable to automate the management, inventory, reporting, and backup tasks. As the network must be redundant and high-available, it means that there must be doubly the amount of each hardware and usually double connections between these equipment. Only that way, we can achieve fault-tolerance and high-available network and the possibility to monitor and manage traffic, events, and logs. To achieve business continuity, all the systems must have support, contracts, and SLA agreed with qualified partners and in addition there must be qualified administrators in house with signed NDA. This is how it is done for the past 10 years. Let's call it a traditional way of doing network security. See Figure 1 for typical high-level design in the border of the network. In the large enterprises there are several borders to the internet and therefore several implementations similar to Figure 1.

The challenges of the traditional way

For the past ten years network and security administrators have been struggling with managing network configuration and security events. There are just too many changing, independent targets in everyday aspects and they seem to grow year after year. That is because the environment changes all the time and devices we are managing are totally independent from each other. So even one single change or event may generate many consequent changes to many single devices' *Access Control Lists* (ACL) and a single ticket may generate several independent tickets to several different internal or external ticketing systems. It is quite complicated to understand the whole picture of the overall network security, because many non-correlated issues and several management products produce different reports which need to be correlated or merged. That is only one attribute of a complicated environment concerning security issues. This is only the administrator's point of view inside the corporation when administration is done mostly in-house. To add more complexity, we can always take into account often needed third parties, supporting parties, end users, and manufacturers supporting tasks. This is especially true, with change management, problem solving, and documentation. The end users use the services and applications that must work end-to-end, but there are quite many network equipment between the ends. So, one single failure in the path usually ends up with service or application doesn't work either partially or at all. Since web based applications seem to grow rapidly, a typical example we need is an updated, modified, or new application to run at the client end that works just a little different way than previous version. If that change needs additional actions in some Layer 4 to Layer 7 network devices like proxy server, load balancer, IPS, or a firewall, that's when the administrator's tasks begin. See Figure 2.

This kind of high-level solution has been installed in many companies long ago, but has it been re-evaluated recently? Was it aligned with business when it was implemented? Management has certainly updated their business and IT strategy in the past years. This kind of solution might have worked well when it was adopted but who does it serve today if not aligned with business anymore? How about the hidden inefficiencies behind the solution that begin to dominate and tend to slow down the IT operations and eventually the whole business? If decision makers don't take advantage of real-life administrators' experiences when adopting the current environment, the business alignment will not be achieved and it will lead to the unrealistic expectations. In the worst case, it will lead to a situation where decision-makers tighten up timetables, money, and resources while demanding more on IT operations. Nobody wins in this kind of situation and more frustrations will arise between departments. This drives IT to choose cheaper, temporary solutions to satisfy the needs more rapidly, but without any long-term results that would eventually serve the business. These are more internal challenges, but there are also external challenges as well. The world, people and company or some of its operations has certainly changed. Applications have been made more complex and dependent of other applications and services. Most of all, the Internet has changed so much that it isn't even recognizable as the same Internet it was 10 years ago. All of those aspects; people, Internet, and company include threats. So, threats have

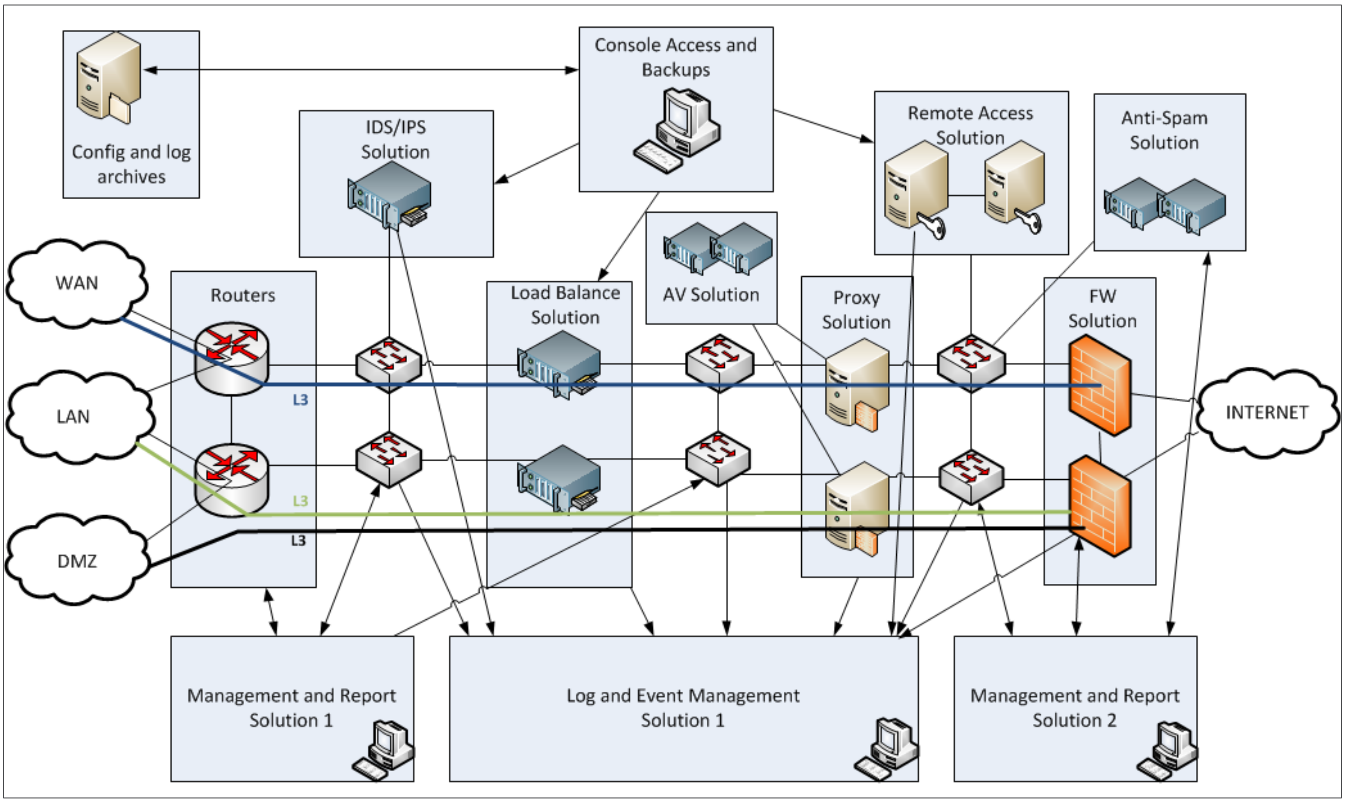


Figure 1. *High-level design of a typical network infrastructure in the border of the network. Black arrows illustrates the flow of events and log entries generated by the device or administrator*

changed. But something seems to be constant and that is the traditional way of doing network security. So, is it a surprise if it just doesn't seem to be sufficient in the constantly changing environment anymore?

Changing environments add complexity and the corporate network and security must adapt to those internal and external changes in addition to align business. The traditional way of doing network security might work well even today, but the nature of the independent network devices defines the capabilities of the whole network. The traditional network has been built up from independent devices that are unaware of the other devices in the network. It therefore resists changes. For example: devices are configured independently; they produce independent log entries many times even repeatedly at the same events. Backups need to be done separately for every device. There are different management and reporting systems since devices run different platforms and operating systems that are mutually incompatible. Devices must be patched since there are different vulnerabilities, bugs, and limitations on different operating systems. Devices are managed by different supporting parties that need regular contract verifications. Troubleshooting is fairly complicated and needs specialists, which might be time-consuming and expensive, especially if outsourced. All of these aspects make the security management complex in the system itself. SLAs must be agreed to the same level for different services with different partners, since end-users applications should work end-to-end with the same SLA. If there is a lower SLA in one device than the other device in the same path, the worst SLA will dominate the whole service level. Licenses might overlap in different devices managed by different partners and cannot be shared or installed between devices (since partners are competitors to each other and competitors do not want to share licenses on others device) causing more license costs to customers, etc.

The list is long and could be continued forever, but they are all features of the traditional way, since the devices were built to be independent. To

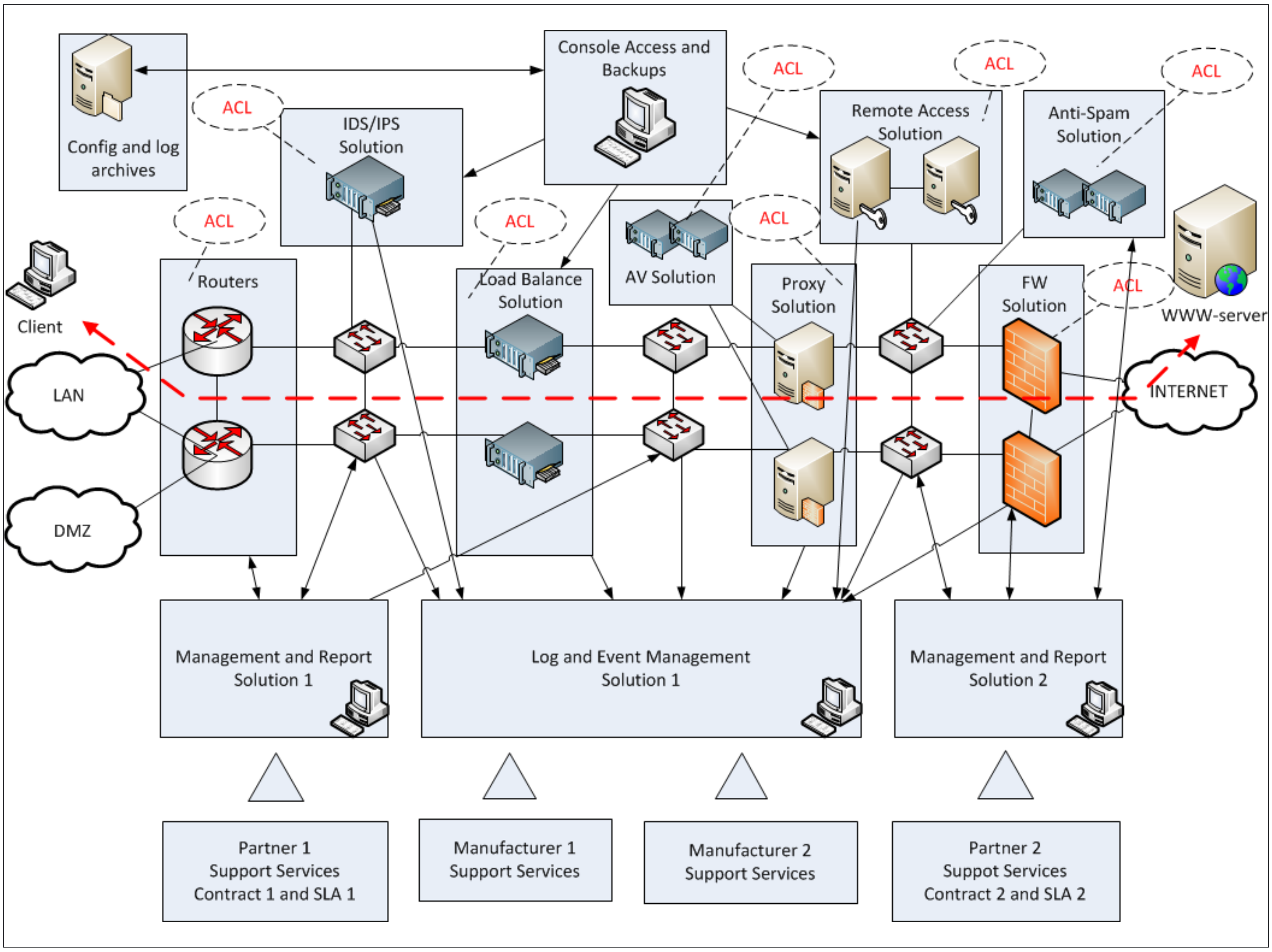

Config and log archives
Console Access and Backups
ACL
ACL
ACL
ACL
IDS/IPS Solution
Remote Access Solution
Anti-Spam Solution
ACL
ACL
ACL
AV Solution
Routers
Load Balance Solution
Proxy Solution
FW Solution
ACL
WWW-server
Client
LAN
INTERNET
DMZ
Management and Report Solution 1
Log and Event Management Solution 1
Management and Report Solution 2
Partner 1 Support Services Contract 1 and SLA 1
Manufacturer 1 Support Services
Manufacturer 2 Support Services
Partner 2 Suppot Services Contract 2 and SLA 2

Figure 2. *End-to-end communication through the border of the network. ACL represents a rule, rulebase, access control list, or other configuration*

achieve continuity, the system must be re-evaluated periodically or upon a bigger internal or external change and responsibility lies more on management level than operational level. In this modular system it's possible to easily replace a module (system, service or device) without affecting the whole system. Possible reasons for changes are a better solution is found, platform, license requirement, or support change issues. So, modularity should facilitate management. Just buy the additional service you need and plug it in. Well, that is only partly true, but now we know that the increased complexity that it entails will stand for the major role. There is one word that would describe the traditional way of handling changes: reactive. We have either created this situation ourselves or grown up within this environment, but should we question all of this, and could there be a better way to do it?

Before the answer, a quick preview

The first five years of 2000s was a time of modularity. Companies were building independent solutions. After that *Unified Threat Management* (UTM) was invented, that combines several solutions into one. Even though the idea itself was excellent, the implementation was a failure for two reasons. The hardware was not quite ready for it, and it was based on the traditional technology that was not meant to be used the way UTM required it to be operated. The implementation leaded to long delays (latencies) and performance problems when more features were enabled or when the rulebases began to grow. So, they could only be used in branch offices because of their smaller amount of traffic. But small-size solutions seemed to be expensive and there was still a needed other solution for the main office. So companies ended up continuing with the traditional way, and some decided to adapt the UTM solutions with excessive computing power to avoid latency caused by inefficiency of the implementation. Either way, this experience may have left a feeling of uncertainty and skepticism to the customers for further improvements of the network security technologies.

For the past five years technology has taken huge steps ahead, especially in the firewall market. The experiences and the idea of the UTM solu-

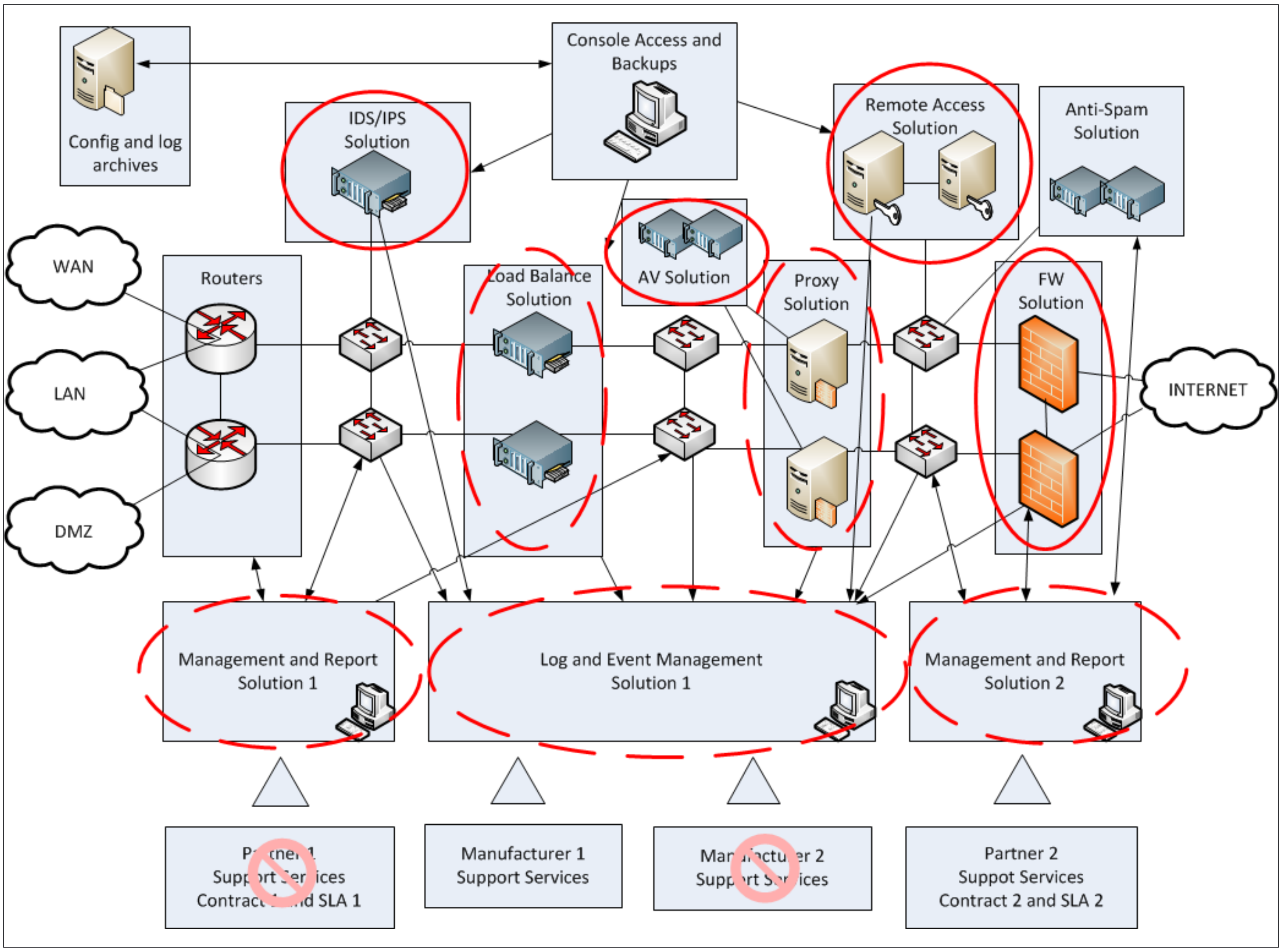

Config and log archives
Console Access and Backups
IDS/IPS Solution
Remote Access Solution
Anti-Spam Solution
AV Solution
WAN
Routers
Load Balance Solution
Proxy Solution
FW Solution
LAN
INTERNET
DMZ
Management and Report Solution 1
Log and Event Management Solution 1
Management and Report Solution 2
P tner 1 Supp rt er ices Contrac nd SLA 1
Manufacturer 1 Support Services
Man acture 2 Supp rt S ices
Partner 2 Suppot Services Contract 2 and SLA 2

Figure 3. *Overlapping or partially overlapping services and network devices*

tion have been taken into account once again and combined with the latest technology – and now the hardware and platform seem to be ready for it. At least one visionary has been bold enough to totally rebuild the FW starting from zero and to build a next-generation network security platform, called *Next-Generation Firewall* (NGFW), refer "Gartner, Magic Quadrant for Enterprise Network Firewalls 2011." This gives the advantage of doing the network security-related tasks with high-performance, purpose-built hardware without the problems of a UTM solution that no other vendor has done – at least not yet. In fact, it seems that all the other manufacturer's firewalls still use the traditional security platforms and/or hardware and that makes the big difference, since they pose the same risk to end up with the same pitfall as UTM did earlier, when implementing advanced technical requirements to the traditional technology. And now follows the answer to the question posed earlier.

Facing the challenges with NGFW

Since there are similarities and overlapping services in the different modules, and the technology has improved for the past years, there is something we can do to improve the overall situation. The overlapping services are marked with red circles in the Figure 3. Partially overlapping (the dotted red circles) means that overlapping depends highly of the existing configuration, services, and purpose of the particular network device at the company.

IDS/IPS, FW, VPN/SSL-VPN, Proxy servers, AV, and load balancers functions in Layers 1-7, depending on how much of their functions are used in the current environment and depending somewhat on the solution itself, they have overlapping properties. Since the environment itself is already complicated enough, administrators tend to keep the configurations simple to avoid even more complex environment and administration tasks. For example: proxies are usually used for authentication, web categorization, antivirus integration for web traffic, blacklisting, whitelisting, and some simple content filtering issues, but rarely complicated reverse proxy policies, SSL encryption/decryption or complex content rewriting. Remote access solutions are usually configured to simply use IPSEC with VPN or SSL-VPN, but rarely for L7 properties in SSL-VPN case. IDS and IPS are usually used with preconfigured settings and less customized or complicated settings and they are implemented either in-line or just monitoring mode. Load balancers are usually implemented to only balance the traffic with desired servers in active-active or fail-over mode with L4 implementation, without doing any additional L7 configuration. However, the configuration varies widely in the enterprises. Since next-generation firewalls can do all, or most of the task mentioned above, it is practical to replace them with one single solution. NGFW offers also wide range of additional services, like DOS prevention, access lists based on AD groups, which can be further combined with application control, country-specific IP groups, or web categories. These features reduces greatly the amount of firewall rules used in day-to-day business, as well as automatically updated threat management, AV, and application identification based on traffic behavior. This way reducing the daily administration tasks can really free resources to other administration tasks without the expense of security. People tend to forget that daily administration tasks are critical in the security point of view and NGFW solution will intensify those tasks through automation. Additional security enhancement is a special functionality, that inspects every administrator defined files from live traffic and sends them in to the cloud which in turn returns a specific report on its behavior and marks them as a malware or not. This behavior affects to all customers using NGFW, so they will be sharing that information through the cloud and helps to protect each other from unwanted software.

By replacing the overlapping services and devices with next-generation firewall, it's possible to simplify and secure the environment. The security enhancement comes with the features that are offered within the same solution, which indeed forms a sophisticated view of the security-related events combined with numerous other events within a single management console. It reveals application, threats, and custom data using predefined (like credit card or social security number -filter) or user-defined regex strings (like "confidential") nearly in wire-speed. QoS can be achieved based on application combined with user groups in AD, for example, instead of certain TCP-ports or interface only. QoS with application identification functionality offers a method to control bandwidth to less important application without the expense of important application by guaranteed bandwidth allocated to important apps and limiting the bandwidth with less important apps. In addition, it not only forms customized network and security related reports and statistics but exports netflow data to existing network management server. This way it can be actually used to form a complete view both network and security. For more customized integration it has an interface to external sources as well, and it can be used together with other devices, such as incompatible with Microsoft AD devices, WLAN controllers, Access Control Servers, or management software. Replacement of the overlapping devices is illustrated in Figure 4.

Implementing NGFW has also additional positive side effects. After replacement, there is less network equipment and therefore it simplifies several management tasks at the operational level. This creates more time for the IT administrators, since they need less time for the same tasks. Also, less equipment usually means a decrease in license costs, since possible overlapping licenses are not divided to multiple partners anymore and some partners are not even needed anymore. Therefore, we can achieve less SLA agreements and contracts. Depending on how many network devices can be completely replaced, the need for SIEM or centralized management and/or centralized event logging system may not be needed anymore, reducing license cost even more. Even if we need them, their license cost can still be reduced, since the amount of data is most likely to be much smaller and some licenses are based on the amount of data or events generated to the SIEM or event management system. Since licenses are handled in the same management location as the NGFW, they are easier to renew in the single place with several services, at the same time and with the same time-period.

Events and monitoring is done in one place, combining them with customized reports, and the security administrator doesn't need to gather the information from several systems anymore. When building high availability with active-active or active-standby solution with double disk on each node, there is almost zero need for backing up the system's configuration or logs. People have commented that in this solution you may have all the eggs in one basket. Well, I don't think so. I would rather mirror only two physical devices (one logical solution) than mirror all the other independent devices (several logical solutions): FW, Proxy, AV, LB, IDS/IPS with mirrored switches, and network connections. This would end up complex network solution and there is always increased risk that failover does not work at some point of the network or configuration mistakes and errors will occur more easily in time. NGFW does not include load balancing, web cache functionality, or WAN accelerator at all. So, these

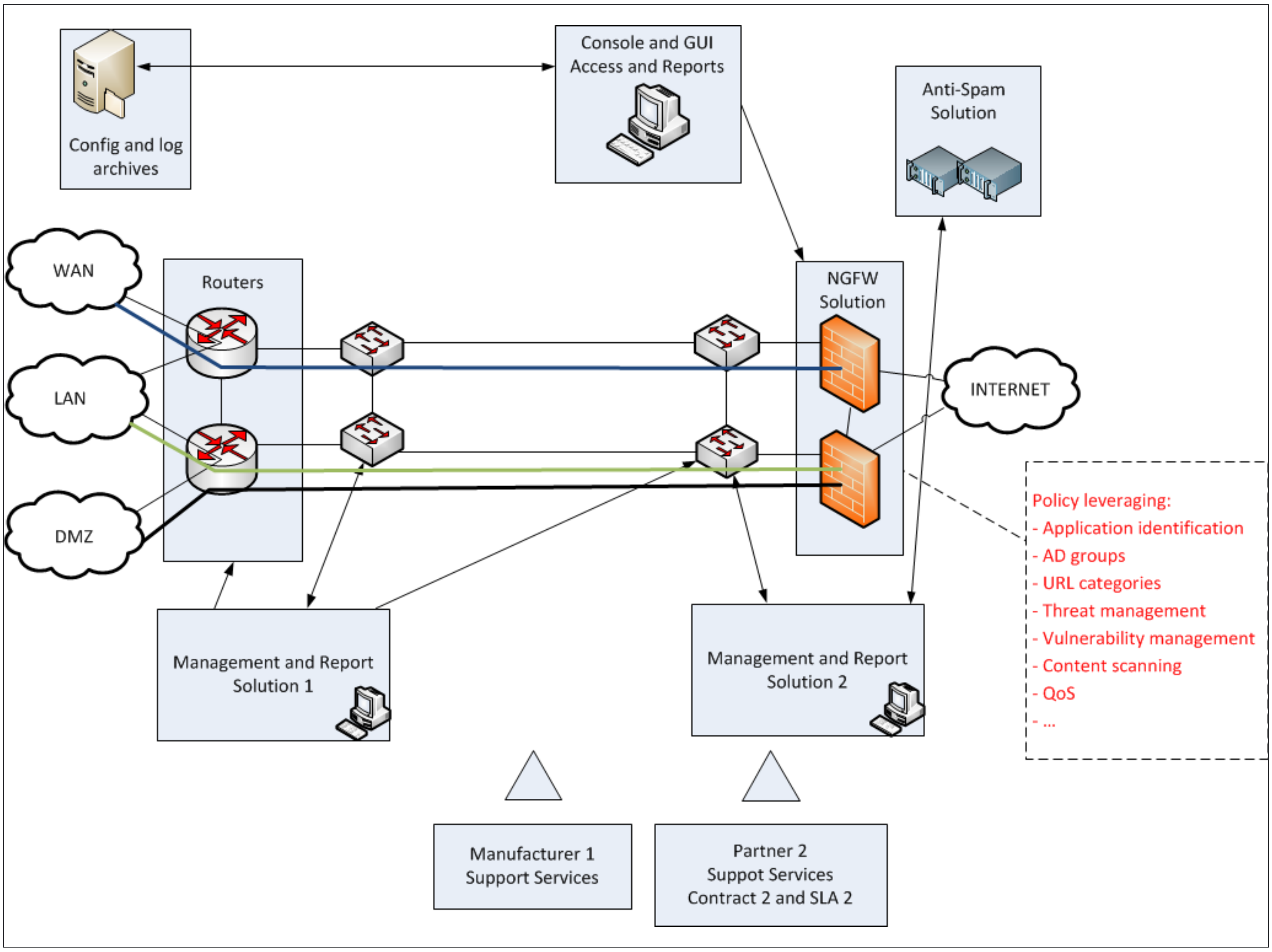

Config and log archives
Console and GUI Access and Reports
Anti-Spam Solution
WAN
Routers
LAN
DMZ
NGFW Solution
INTERNET
Policy leveraging:
- Application identification
- AD groups
- URL categories
- Threat management
- Vulnerability management
- Content scanning
- QoS
- ...
Management and Report Solution 1
Management and Report Solution 2
Manufacturer 1 Support Services
Partner 2 Support Services Contract 2 and SLA 2

Figure 4. *NGFW solution replaced to perform IDS/IPS, AV, FW, IPSEC-VPN, VPN L2L, Threat management, Application identification, URL Categorization, User access control with AD, QoS, and DOS Protection*

functions must be added with external devices or not have them at all. I remember that caching was very useful when it was introduced many years ago and it saved internet bandwidth even up to 50%. In my experience during the past years, using caching in web browsing saves only approximately 15-20% of the total internet bandwidth, so its existence may not be justified, since Internet capacity is cheaper than plain cache service. But this also varies a lot in companies, since they use Internet and proxy servers in different ways and for different purposes. The reason for degradation might be the increasing use of mobile devices, which may be more and more connected to other than corporate network. Since mobility has been increased, it also means that people working hours are different than just office hours. That can explain why internet bandwidth usage may be divided through a longer scale, instead of just office hours. It also means that during the peak hours internet bandwidth is more flattened and that's why internet capacity may be smaller and more constant. Therefore, the cache's efficiency is smaller, because one of the cache's advantages is to serve internet content from the cache, especially in peak hours. Internet content is also more dynamic, encrypted, and password protected that are all non-cacheable features. WAN accelerator and load balance are not so much border network services, but rather WAN and server network services that should be still used there. So, if we can replace the overlapping services in the border of the network, those resources are freed up to be used in the internal network. For example, load balance is not needed anymore to the proxy traffic or AV traffic, if they are replaced.

Changing the FW to the NGFW is not so different from changing whatever firewall to another FW. The basic steps are the same and the topology usually changes somewhat. Configuration is cloned using automated tools and manual configuration is always partially needed. Cloning usually clones objects, FW rulebases, and NAT rules. FW and NAT rulebases must go through manually and make necessary changes according to new topology. The biggest relief is the new rulebase matrix. In my experience, NGFW usually reduces FW rulebase from 25% to 75%. And that is, since in the traditional way you enter a source IP/mask, destination IP/mask and port/protocol to add one single rule. In the NGFW, you can replace them with AD groups, URL categories and applications, that all consists of those many single objects: DNS name, IP addresses, URL addresses, etc. So, controlling one level higher, you can still control those single objects, but management is far easier. In addition, these rules affect to larger user and object groups, which means that they replace many single rules and they don't have to be edited so often. And that is, since AD groups are edited by appropriate owner or administrator, and because applications, web categories, threat management, and AV signatures are all dynamically updated and enabled in the rules. Routing table should enter manually and verify overlapping entries. VPN L2L tunnels should be configured manually and verify active tunnels that really exist and still needed. Network segmentation should be re-evaluated, since NGFW can be easily deployed between servers, DMZs, and office networks using routing or virtual wire capabilities. This way threats, unwanted programs, and applications can be controlled and combined with AD groups without need for complicated and time consuming traditional FW access lists (see Figure 2). After FW has been replaced, additional features can be activated one by one. Like SSL decryption/encryption based on categories, BYOD, location aware VPN Clients, reporting, and trend analyzing. This way true NGFW functionality is possible, and the advantages should be seen quite soon after installation. There is also one word that would describe the traditional way of handling changes: proactive. For some reason IT tends to drift to the role of police, but it is not possible to control business when the business knowledge is inside the business departments. Therefore, either the business representative must do some of the administrations tasks or IT must do in-depth co-operation with business departments. So, if AD group management is done by every business units for its part, then it's a perfect example of using that information in the FW policies, since business units knows who are in what roles and should be in what AD groups. Of course, business unit representatives can be only in an authoritative position and AD management is done by other unit like IT support level 1 as well. Either way, this is to everybody's benefit, instead of a battle who should be controlled and what. This way we are heading in the right way in business alignment between departments and IT operations and the changes will also take affect more rapidly.

Whenever a firewall is tested in a *Proof of Concept* (POC) phase by the company, it is critical that customers enable simultaneously as many features as possible, with at least current traffic amount of real traffic, including VoIP (prioritized) traffic in order to make the right choice among firewall vendors and models. During tests, it is important to notice that the resources of the firewall increase only by percentages or tens of percentages when traffic increases or doubles. This can be used to estimate how much the increased traffic amount affects the resource consumption. That gives more confidence that the solution lasts more than just the near future, and does not fail right after production phase when the live traffic enters the device or is increased with double amount of traffic or sessions afterwards. The quality of the prioritized traffic should never degrade even when most of the firewall features are enabled. That can be verified by constantly monitoring VoIP traffic that is prone to latency.

Summary

It is clear that there is no turning back after NGFW replacement, since it opens up so many possibilities for the future and addresses modern threats in a modern way that really lasts long and aligns with business needs. It offers a possibility for a company to enter a proactive state of managing IT related issues and support business. A big part of network and security related issues resides in the infrastructure level, and NGFW reinforces part that, but also complements IT operations. It therefore affects and leverages directly to a variety of business needs. The more services are replaced by the NGFW, the more easily it responds to the following:

- faster response time for many IT related changes between IT operations and other departments
- less dependencies and uncertainties between different systems and their configurations
- simplifies different services and systems including configurations, change management, and trouble-shooting
- intensifies IT security handling by comprehensive security monitoring and reporting
- enables IT operations to align with business needs and changes

PAULI LAINE

Pauli Laine, CISSP, CISA, CISM, CRISC has been working as a network and security specialist since 2001 in several companies in retail, insurance, and construction companies in Finland. His responsibilities has been included a wide range of network and security devices, security related issues and incidents, including network and security reporting, monitoring and internal security task forces. He has been involved many firewall replacement projects, network architectural designs, and implementations including remote access systems with strong authentication systems. Pauli works in a global construction company, NCC Construction in Finland.

Proposed Security

Enhancements to the 802.11 Protocol and Wireless Routers

Protocol designers are faced with many challenges due to the problems with wireless network security. As you may know there are many tools out there that allow for WPA/WPA2 and WEP decryption, which pose a threat to all wireless network users. How can we fix that?

What you will learn…

- What are the proposed enhancements to make wireless networking more secure
- Why our data has been poorly secured and encrypted
- How to protect yourself while using wireless routers

What you should know…

- Wireless Network Security basics

This article will discuss the proposed security enhancements to make wireless networking more secure.

The Current Problems with Wireless Network Security

There are many obvious problems with wireless network security that bring challenges to the protocol designer. This article proposes ways to mitigate an injected management frame attack and how we can add extra QoS features to wireless access points. Packet injection is an attack in which an attacker injects frames into the network at the link layer causing it to respond and act in his or her favor. This is due to the fact that even though all of your data may be encrypted using WPA/WPA2 and WEP encryption, the frames that are used to "manage" your network are not and can be forged arbitrarily.

Not many of us even use WPA or WPA2 anymore, which, at the time of this publication, is standard. Recently, I took a broad statistical analysis of SOHO and residential wireless networks and noticed that there is almost as many open or WEP encrypted networks as there are with WPA and WPA2. Open wireless networks are obviously the easiest possible way to have your information placed into an attacker's hands. Hiding your ESSID or name of the wireless network only creates a small speed bump for even a novice wireless hacker. Using a MAC address filter is even a bad method of securing your wireless network, as MACs can be easily spoofed by an attacker with simple UNIX networking tools. WEP encryption was technically broken in the year 2001 when Fluhrer, Mantin, and Shamir showed that the first few bytes of the keystream literally "leaked" the key. Since then, the RC4 (used by WEP) method was leaked into Cypherpunk's mailing list and is no longer a trade secret, and Aircrack 1.0 was released in 2004 based off of work from David Hulton's dwepcrack.

Q. So, why do we still rely on poor encryption and security of our data if we've had access to these tools for over 8 years now?

This shows that we are very slow to adapt new security measures for wireless networks.

Frames are divided into three categories in 802.11. They are the Control frames, Management frames, and Data frames. Control frames are used to control the sending and receiving of packets. Management frames are used for synchronization, information, and authentication. Data frames are for our precious data and also include network protocols such as ICMP, ARP, and IP.

In computer science, there exists a set of instructions to allow a network adapter to "inject" frames into a network while in promiscuous mode. These sets of instructions are built as libraries in programming languages and can be used to quickly write an application in which we inject frames into a network. Most 802.11 administration and penetration testing software, including Aircrack-ng, use these libraries to monitor packets or transmit them at the link layer of the network.

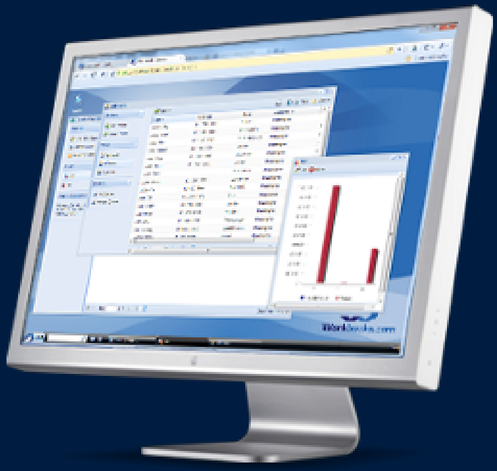
Q. But why would we want to inject frames into a network?

Well, to recover hidden ESSIDs, for example. When we drop a user's connection to an AP in which the ESSID has been hidden, the probe request packet to rejoin the network sent by the supplicant software, contains the ESSID in plain text. Any simple 802.11 protocol analyzer could then view it. We could also generate ARP traffic to control the network into giving us more of those first bytes that leak the WEP key. Once connected to a victim network, we can even inject frames to pretend that we are the authenticator to the supplicant and perform either a Man-in-the-Middle attack, or an advanced WPA2 Enterprise phishing attack. We can also generate probe requests in which an AP must respond to at a fast rate jamming up the 802.11 channel.

In WPA2-enabled wireless networks the management frames, which includes the deauthentication and disassociation frame sets, are not encrypted. These are what attackers use to gain unauthorized access to wireless networks. Using the libpcap C library, we can write a simple UNIX C application to specify which client MAC address we want to deauthenticate from the wireless network with our wireless radio in promiscuous mode. Once deauthenticated from the AP using these specially crafted disassociation packets, the supplicant, or station machine, will again attempt to reautheticate to the authenticator. This generates the "4 way handshake" process in which we can then capture the traffic for an offline dictionary, or brute force, attack. This is a drive-by attack method which is far more common than a long term packet monitoring attack on a company. This is not news. The Aircrack Suite implemented packet injection with aireplay back in August of 2004.

Q. So if they are open to anyone and we are completely exposed to being spoofed, how can we protect ourselves?

At the MAC, or Media Access Controller layer, an experimental possibility exists. The attacker forges 128 frames and sends them to our client machine.



This client machine then drops its connection to the AP. How can we stop this from happening? Well, we can simply check the power levels of the previous frames sent by our actual AP. If we were to use the driver software and the radio to store a small (or large, depending on our threshold) array of integers that get compared using simple statements, we can drop an attackers frames and mitigate the attempt to deauthenticate our client.

The chances that an attacker's frames are of the same power quality as our valid AP are slim in most cases. During our normal engagement with the AP, we can set a simple timing interval which starts and stops the reading mechanism. There already exists a timer function and carrier energy sense in mostly all code for 802.11 drivers which implement WPA2 for the MIC, or Michael Integrity Check. This reading function in the correlator will take the received power levels in several sequential packets, specified by our threshold (let's call this our "security threshold"), map their reception to integers, and create a list. The next time, Deauthetication-specific Management frames come from our AP to us without our request, we can match their power levels to those in our list. This will prevent packets from making it up the networking stack at the very base. If we were to implement this method into the AP itself, we could mitigate evil twin or spoofing attacks made by illegitimate clients.

A true radio denial of service attack will simply transmit a constant signal on an 802.11 sanctioned frequency, or "channel." This constant stream of "noise" will deter radios from transmitting because, well, they are polite. The 802.11 protocol specifies that a radio must wait its turn using a "request to send, clear to send" method. In turn, the radio's driver software determines which packets are sent using this method by their size. This only pertains to unicast frames, or frames that are sent to a specific destination. This is why an ARP, or Address Resolution Protocol, replay attack is possible. ARP frames are "broadcast" frames, which are sent out to everyone in the network on the medium radio frequency (RF) without request. With this in mind, we can, however, keep a constant watch on any 802.11 frequency set using a simple $30 USD USB spectrum analyzer added to our wireless access point. Our AP can check the analyzer's output during the same intervals used by our reading mechanism to check for constant noise levels. If noise levels are found, we can forge a multicast set of frames and send them to our clients to change to a clearer channel. Also an Ethernet device can be modified in the AP's UNIX-like firmware to watch for a massive amount of ARP requests within a certain time frame. If detected, it could also trigger this new mechanism in the AP to change channels, shutdown, or even use mail to send the administrators an alert message.

If our client laptops were to move freely among the AP's radio aperture, this movement will remain gradual. In an industrial or medical environment, a wireless desktop adapter would remain mostly at a constant power threshold. Thus, if our readings by the correlation reception code were running, we would see a set of power levels that appeared to be linear. If an attacker outside of our set attempts to inject frames that were close to our set of integers, we could still detect that they are malicious using longer-term statistical analysis. If the reception power of the frame were to change drastically, from say, attenuation, at the time of deauthentication, this could prove a false positive and frames will be dropped. Deterring these attacks does not improve the quality of security that is flawed by the WPA2 encryption algorithm, but protects from any external malicious influence. If implemented, tested and finely tuned with a stationary wireless client, we could even mitigate from an attacker injecting frames on an open network spoofed as legitimate MAC addresses and man in the middle attacks.

This method could also potentially deter extensive long-term attacks. Since WPA2 is flawed and it only takes a simple 802.11 protocol analyzer to detect its weak spot, an attacker monitoring for a long enough period could still get this data without injecting a single frame. If the WPA pass phrase were compromised using this method of offline dictionary attack, the attacker still would not be able to spoof as the legitimate client and authenticate to the network if his or her power levels to the AP were out of its security threshold.

Q. What If the attacker were to wait until our legitimate client left the BSS to join?

We could create a new web interface to the AP which we could access with our 3G/4G devices to turn off and on access to clients using simple IPtables settings. Then, the user can login to it and allow the MAC address to connect.

In conclusion, there exist a few possibilities to deter 802.11 denial-of-service and intrusion attacks that could be implemented. This would require an amendment to the 802.11 protocol as added broadcast packets will need to be designed and the radio drivers would also need altered but could prove useful to securing our wireless data.

DOUGLAS BERDEAUX

Douglas Berdeaux is a founder of WeakNet Laboratories, you can contact him via weaknetlabs@gmail.com

Get the best real-world Android training anywhere!

Attend

AnDevCon IV

The Android Developer Conference

December 4-7, 2012

San Francisco Bay Area

Choose from more than 65 classes and workshops!

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

- Learn from the top Android experts, including speakers straight from Google!
- Attend sessions that cover app development, deployment, management, design and more
- Network and connect with hundreds of experienced developers and engineers like yourself

Register Early and SAVE BIG!

www.AnDevCon.com

Follow us: twitter.com/AnDevCon

> "AnDevCon is a fantastic conference! There is no better place to experience the latest and greatest technologies and techniques in the field of Android development. If you attend one conference this year, this one should be it!"
>
> —Jay Dellinger, Senior Software Engineer, Manheim

A BZ Media Event

NetFlow

information to track network events

What is NetFlow and How to use its information to track network events? This article will attempt to teach you about NetFlow, but be warned! You need to realize that this solution has numerous merits, it cannot be used as a cure-all to the situations you may experience, but it is a very useful adjunct to your toolkit.

What you will learn…

- How NetFlows are generated
- Sampling rates can be used to reduce CPU loads
- fingerprints can be shared amongst users
- anomaly reports can help detect malicious traffic
- types of data objects that can be tracked
- report generation
- NetFlow version characteristics

What you should know…

- Basic knowledge of routing protocols
- Knowledge of the TCP/IP stack
- Experience in packet capture interpretation would be useful
- Network security mindset.

Imagine if you will, a peaceful night's sleep interrupted by a pager beeping, telephone calls and confused operators trying to describe what is happening in the network and as you slowly wake up and try to log on to your laptop, you realize that all your preparations and hard work deployed in the previous months wetre worth it as you are able to have a high level view of the situation and even know which type of traffic and origin of the malicious traffic.

Within minutes, you can have an access list applied to your devices or even a BGP black holing statement issued to take care of the problem. The operators are amazed at the speed and ease with which you were able to resolve the issue and you even have nice graphs and reports produced about the event that the higher management will need to see, the next day, as they will question you about what happened and how to mitigate such events.

This is all happening because you implemented NetFlow collectors and a controller in your network and created a baseline about the normal traffic patterns. Your next step is to train the operators to do the same tasks so you won't have your sleep interrupted, in case it happens again.

Continuous monitoring may not be necessary if you program alerts to be sent via email or pager calls sent, once filtering on high alert settings with a duration threshold reached, for instance or by initiating a SNMP trap to alert the network administrators.

- Is this sounding too good to be true ? Not at all, these actions occur on a regular basis and new
- techniques and procedures are produced as time goes by and as the experience level grows or
- new features are introduced by the NetFlow device manufacturers.

The following article can be used as a starting point and is not intended to be a full recipe to manage network events, network device and NetFlow collector manufacturers have further descriptions and data sheets about their offerings, if you so choose to go ahead in implementing NetFlow collection in your network, by using commercial solutions as this will permit a faster deployment and the learning curve will be smoother.

You need to realize, though the solution has numerous merits, it cannot be used as a cure-all to the situations you may experience, but it is a very useful adjunct to your toolkit.

We will therefore describe suggested arrangements and try to describe various elements that are either part of the issues or the solution, this will give you a good starting point and hopefully guide you towards establishing the ideal situation and reduce the number of catastrophic events that may occur on a more or less regular basis.

Network Management

In order to be able to protect your network, there are a few techniques to make the task a bit more easier and help us focus our attention and resources in the right direction.

Although we should not rely on any one tool or technique to do the work, NetFlows along with active and passive DNS, data captures, information exchanges within a network security community, ingress and egress filtering, DDOS mitigation techniques such as access list filtering or BGP black holing or even diverting the traffic to packet scrubber devices should be sufficient to handle most of the events encountered during regular operations.

What is NetFlow ?

A NetFlow packet is usually generated from a router or a switch processing traffic and generating NetFlow packets containing several values about various parameters that are part of the data packets transiting the interfaces under scrutiny.

Various manufacturers will have Jflow, Cflow or Sflow equivalents to NetFlow and their documentation can provide specific information on how to configure and use the flows generated. We will use the term NetFlow in this article as a generic designation for all types of variants mentioned above.

Keep in mind that some of the capabilities and details would not be supported in some flavors of NetFlow equivalents or not in the same format.

This protocol can be used to perform network and security monitoring as well as network capacity planning, ip accounting and traffic analysis.

Depending on the platform used and the ip version (ipv4 or ipv6), the NetFlow version will vary and may contain more or less of the interesting data contained in the NetFlow packets.

Typically, these packets are forwarded to a collector using the UDP protocol with a particular port designated along with a sampling rate and direction of capture, software programs are used to generate reports and track conversations between the targeted ip addresses and its remote connections. Some platforms support SCTP reliable exporting of these flows. These flows can enable you to track misuse on your network or track specific patterns or protocols.

Another use is to detect traffic that exceeds the usual volume of traffic destined to an interface or ip address, some platforms would contain applications with built-in signatures that will detect and report malicious traffic.

Yet another way to track specific flows is to use the fingerprinting capability by specifying a trigger rate or a signature (TCPdump syntax) These fingerprints are created from events that are specific to the conditions seen or searched from the system and can be shared with other users.

NetFlow versions

The most prevalent versions are v5 or v9, although we can find versions such as v7 or v8 on some platforms.

Versions 5 & 9 will typically carry the following information fields:

- Source address
- Destination address
- Source port
- Destination port
- Protocol type
- Input logical interface
- Output logical interface
- TOS field
- AS name
- TCP flag
- MPLS label (v9)
- MPLS label type (v9)

Version 5 is the type mostly encountered and has a fixed export format whereas version 9 has a flexible export format and is the basis for the IETF Ipfix protocol. This version is mostly used in newer generations of network devices. (*http://datatracker.ietf.org/wg/ipfix/charter/*).

Even if you do not export these flows to a collector, they can still be useful in tracking activity within the router or switch internally and can show you the top ten talkers, for instance or anomalies affecting your devices, but if you use NetFlows in this manner, just ensure that you turn off the NetFlow generation process within the device when you are done as this will impact the resources of the device, Built-in show commands are usually part of the operating system being used within the device.

It must be understood that NetFlows being generated should be one of the several tools at your disposal to monitor, detect and capture malicious traffic transiting your network, then data captures can validate and provide useful information about this traffic, for traceback or forensic uses, for instance

Sampling rates

Sampling rates can be specified to be 1 to 1 or 1 to ten thousand and everything in between the above values, meaning either one NetFlow packet generated for every data packet crossing the inspected interface up to one NetFlow packet to ten thousand data packets, impacting the CPU cycles accordingly IE: 1:1000 would impact the router cycles much less than a 1:10 configuration.

Always monitor the CPU loading before and after enabling NetFlow generation.

Some applications will also do sampled data captures as high capacity links can easily overwhelm monitoring platforms. The same NetFlow packets can be shared with several applications that can do storage, billing, accounting capacity planning or visual representations in order to better comprehend what goes on within your network.

Collector placement

We should deploy NetFlow at the edge of networks, for instance, or aggregation points to better characterize the traffic flows. Data centers can also benefit from NetFlow analysis (Figure 1). Alternate network design (Fugure 2).

Network Capacity Planning

NetFlows can simply be used to monitor links and applications present on your network in order to plan ahead and add capacity to links for instance, it can also serve as an ip accounting application for peering or transit agreements or for billing purposes.

Another nice feature that is usually part of the capabilities of NetFlow collectors is to store information about events in a database to be able to retrieve historical data and to document trends.

Other protocols can supplement the information gathered with NetFlows such as SNMP, Syslogs, IDS alerts and monitoring, active or passive DNS and data captures where available would provide the granularity required when dealing with a particular threat.

Generating a baseline

Using NetFlows would enable us to perform a baseline of network traffic to be referenced, in case of an DOS attack or unusual event occurring, this data will be very useful to enable specific actions to mitigate malicious traffic.

Open source solutions are available to get you started at little cost but you will need to spend some time setting up your system to collect and analyze the data collected, commercial offerings will allow you to profit from the manufacturer's expertise and experience in setting up your system, at a cost, but it usually comes with pre-configured reports and analysis tools as well as fingerprint creation functions. Once your baseline is created, profiles can

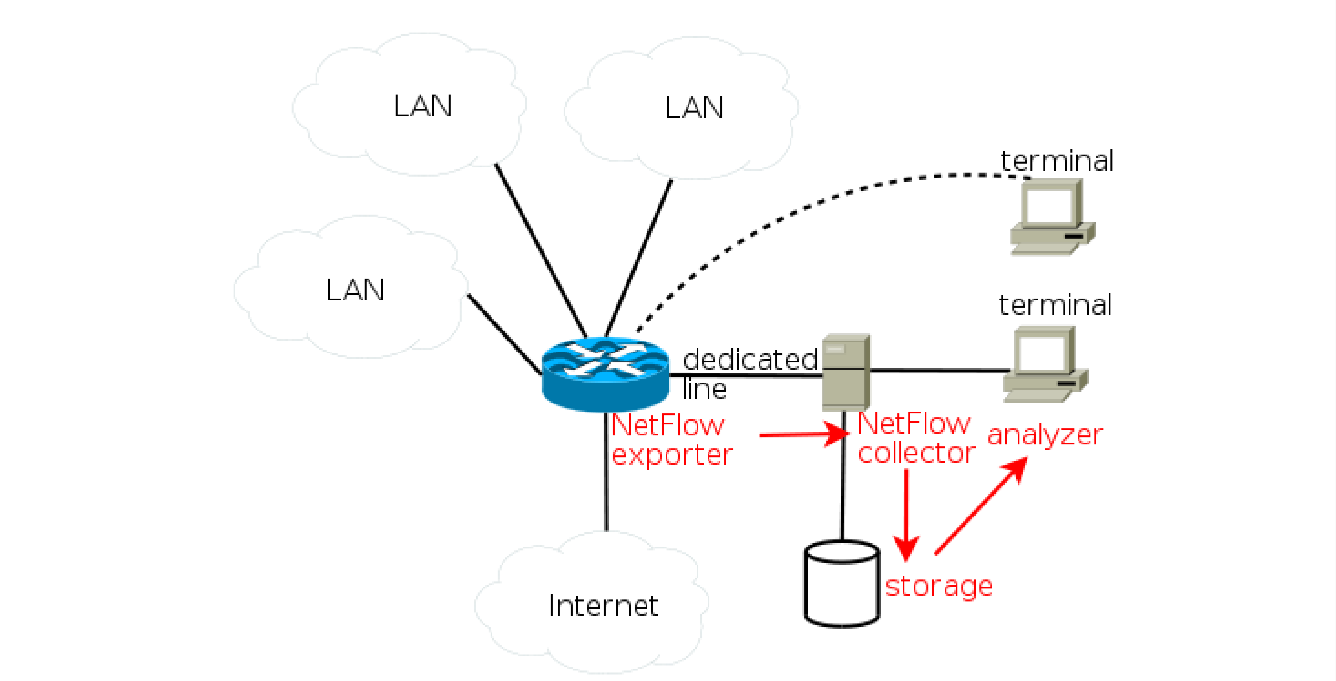


Figure 1. *NetFlow Architecture, diagram from Wikipedia by Pazder*

be established and serve as tracking points or elements used as managed objects or fingerprint input criteria.

The NetFlow devices can also track routing instability within your network and will alert you if you encounter misconfigurations or peering anomalies.

Classifying anomalies

We also need to adjust sensitivity levels to detect and classify anomalies as low, medium or high severities.

The classification of these alerts are dependent on several conditions such as trigger rates, event duration or threat patterns.

A combination of patterns such as TCP SYN traffic at a high volume during a few minutes would trigger a High Alert .

Also the number of routers and interfaces involved would also influence the classification of these alerts. This system would enable the network administrator to visualize the event and take appropriate measures such as applying an access list for instance or generate a BGP route injection either manually or via the monitoring console or application.

Denial Of Service Attack

What is a Denial Of Service attack?

An attempt to overwhelm resources either of the network provider or the end users thus affecting network capacity or availability and if the attack is distributed, the effects would be amplified and the collateral damage can we worse than the initial impact.

Types of malicious traffic

The following list contains some of the attack vectors.

Traffic rates towards specific hosts that deviate from normal internet practices as is often seen on the Internet to paralyze a company's operations or even the network provider's devices.

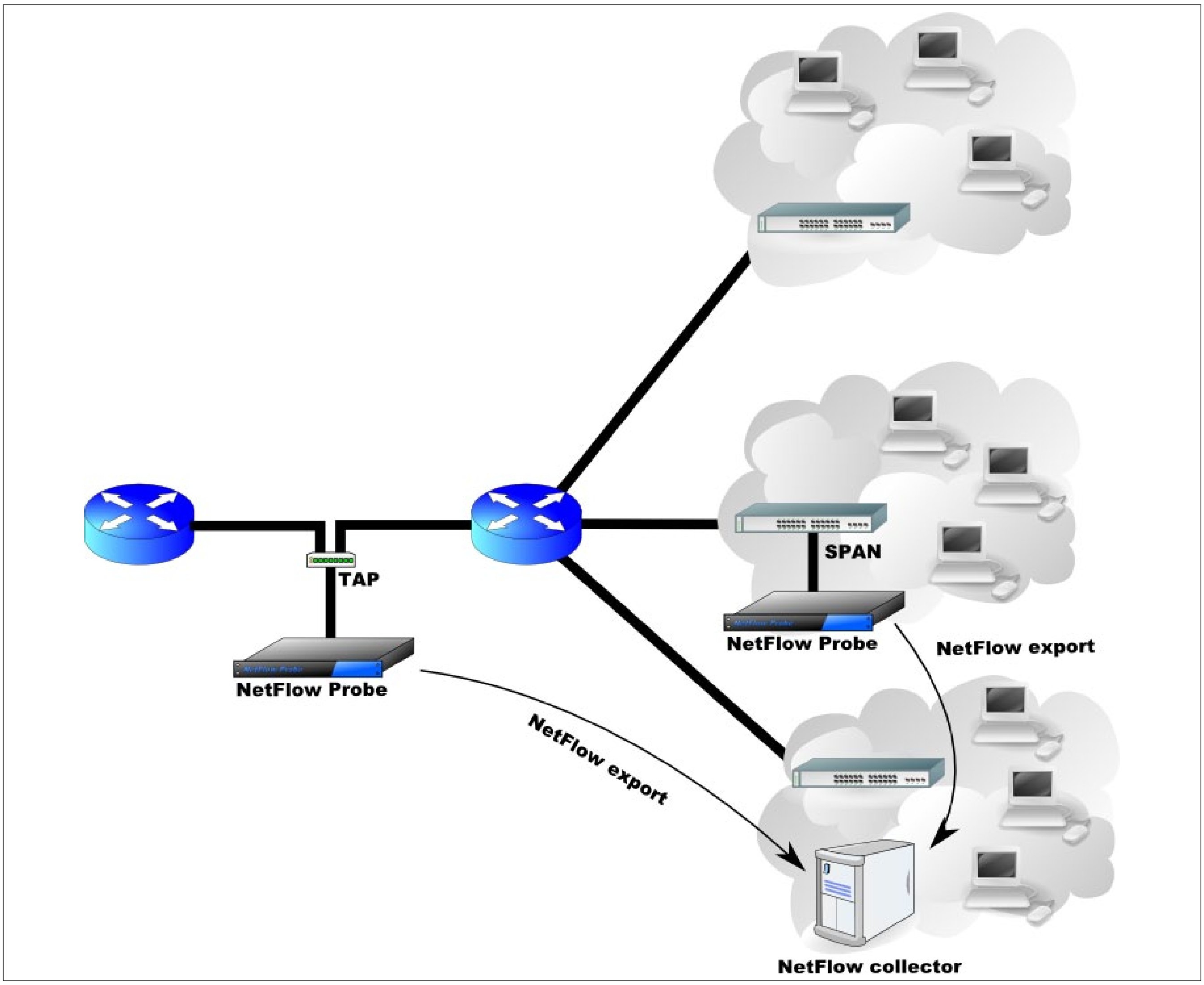


Figure 2. *NetFlow architecture using standalone probes, by helix84 from Wikipedia*

Misuse anomalies cover the following types of traffic

- icmp anomaly (ICMP types and data rates)
- tcp null flag anomaly (mostly scanning activity)
- tcp syn flag anomaly (flooding rate)
- tcp rst flag anomaly (flooding rate)
- ip null (protocol 0) anomaly (flooding rate)
- ip fragmentation anomaly (flooding rate)
- ip private address space anomaly (spoofed traffic and rate)

dns (tcp and udp port 53) anomaly (flooding rate)

total traffic bps and pps deployed against common attacks targeted at individual network hosts including syn, smurf, fraggle (well known attack signatures).

Mitigation Techniques

You can help defend against spoofed traffic by filtering ingress and egress traffic streams by using different techniques (bogon filtering, urpf....etc...)

Commercial units would also create anomaly-specific access lists to counter that particular event, these access lists can be customized to work on specific devices or across your network and in a format type recognized by different router brands. They can also generate black holing BGP announcements towards border routers.

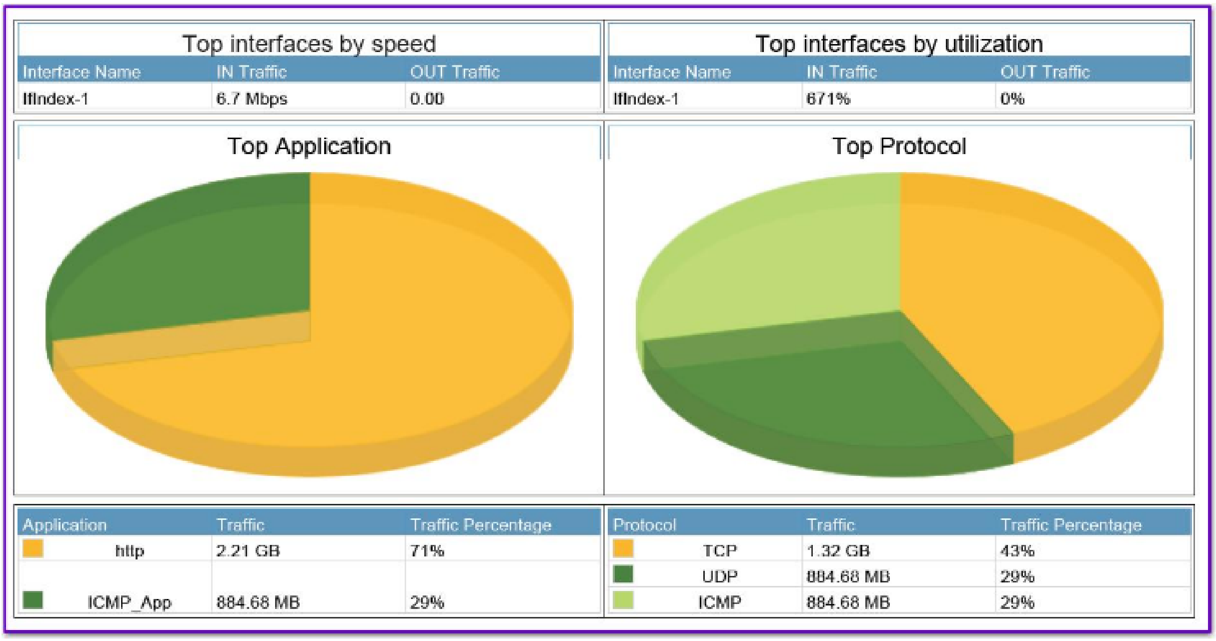
You first create a BGP route such as 192.168.1.1 with a next hop of 192.0.2.1 with a no_export community to ensure the routing instruction does not leave the Autonomous System, then on the edge routers a static route stating 192.0.2.1 goes to Null0, thus the final result is that traffic directed to the prepared ip address will be blackholed at the edge routers

When you have a source ip address or a list of addresses to blackhole, you then direct that traffic to the BGP route described above and within a minute, all borders routers should have the modified routing information. This can be done manually or from within the NetFlow device or the application.

Report Generation

From within the NetFlow controller's application or console, you can zero in a particular alert or severity pattern and generate a report that could be a high level description of the event, but also gives you the possibility to drill down to a second or third level of details to better comprehend the attack, impact of such events.An example of second level of details can show subnets involved and to what degree, whereas a third level may indicate FQDN and "Who Is" information about the hosts involved.

You could also generate reports based on your own created fingerprint or from a shared fingerprint to track a particular protocol and who uses it within your network or see connections talking to a specific host, for instance. Another type of report can be created simply to outline the current state of traffic across the network and used for capacity planning or for accounting purposes as well as tracking other autonomous systems flows across our network. Other reports can give you a big pic-



Top interfaces by speed

Interface Name	IN Traffic	OUT Traffic
IfIndex-1	6.7 Mbps	0.00

Top interfaces by utilization

Interface Name	IN Traffic	OUT Traffic
IfIndex-1	671%	0%

Application		Traffic	Traffic Percentage
🟧	http	2.21 GB	71%
🟩	ICMP_App	884.68 MB	29%

Protocol		Traffic	Traffic Percentage
🟧	TCP	1.32 GB	43%
🟩	UDP	884.68 MB	29%
🟨	ICMP	884.68 MB	29%

Figure 3. *Sample Report – Netflow*

On the Web

- *http://en.wikipedia.org/wiki/NetFlow* – Good description of NetFlows and associated topics
- *http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml* – ICMP types listing
- *http://en.wikipedia.org/wiki/Transmission_Control_Protocol* – TCP description
- *http://en.wikipedia.org/wiki/User_Datagram_Protocol* – UDP description
- *http://en.wikipedia.org/wiki/Border_Gateway_Protocol* – BGP Decryption
- *http://en.wikipedia.org/wiki/Bogon_(address)* – Bogon Description
- *http://en.wikipedia.org/wiki/Ddos#Distributed_attack* – DOS & DDOS Description
- *http://en.wikipedia.org/wiki/Domain_Name_System* – DNS Description
- *http://en.wikipedia.org/wiki/Fqd*n – FQDN Description
- *http://en.wikipedia.org/wiki/Intrusion_Detection_System* – IDS Description
- *http://en.wikipedia.org/wiki/SCTP* – SCTP Description
- *http://en.wikipedia.org/wiki/Snmp* – SNMP Description
- *http://en.wikipedia.org/wiki/Syslog* – Syslog Description
- *http://en.wikipedia.org/wiki/URPF* – URPF Description

Glossary

- BGP – Border Gateway Protocol
- Bogon – Bogus Ip Address
- DDOS – Distributed Denial Of Service
- DNS – Domain Name System
- DOS – Denial Of Service
- FQDN – Fully Qualified Domain Name
- IDS – Intrusion Detection System
- SCTP – Stream Control Transmission Protocol
- SNMP – Simple Network Management Protocol
- SYSLOG – System Logging
- TCP – Transmission Control Protocol
- UDP – User Datagram Protocol
- URPF – Unicast Reverse Path Forwarding

ture about bandwidth hogging applications such as video traffic as an example. Yet another type of report is generated by using the built in dos signatures that are part of many NetFlow devices to track well known malware activity like slammer... etc...

Specific customer profiles can also be created to track their activities and events and thus could be formatted to present them during status meetings. An example of a simple report can be seen Figure 3.

Summary

If one network team or individual has benefited from this article, then the author would have reached his goal. To implement such a structure is not easy, a lot of canvassing teams and individuals in various departments can be tedious, the analyzing of your network topology can be daunting, but I assure you, the benefits are well worth the efforts as the author discovered over several years of overseeing the NetFlow based administrative duties.

It is important not to panic if a catastrophic event occurs as you won't be of any use to your colleagues and cannot think clearly in order to analyze and suggest a mitigation effort.

Establish a network of key people that can help you and to whom you can also return the favor, keeping abreast of new developments in malicious traffic techniques is also recommended. Training sessions that can increase your knowledge and confidence level are not to be overlooked. Once you are ready, then you can provide training to other participants in your project. If you are already involved in network management or operational management, you have the necessary basic skills to investigate if this tool is useful and pertinent to your day to day operations or planned endeavors.

The end goal is to reach a point where your infrastructure will be protected and the end users will benefit from this state and although you cannot block every attempt or anticipate all future forms of malicious activity, you can be as prepared as possible with a good model of defense in depth and to present yourself as a difficult target rather than an easy victim, so NetFlow processing is a very good way to prepare for this and to monitor if you are successful.

CLAUDE LABBE

The author has worked for over 30 years for a large Internet service provider in various capacity, retiring as a network security manager involved in creating and administrating a large NetFlow deployment and is now a freelance contractor as a network support engineer.

The Meta Network

Security Strategy – Another way of thinking

Today, network security has more than ever been associated with high economic costs and extreme technical complexity, which it can be in some aspects. But fundamentally it is really about creative thinking, cooperation within the business and good old common sense.

What you will learn…

- The Meta-Network Security Strategy
- How to align IT operations with business needs according to the strategy
- How to measure your actions

What you should know…

- Basic network security issues

The focus of this article will be on how to think and make a holistic strategy in terms of how to think, before, while and after building a flexible network security platform. Many big vendors, have courses, products and strategies for how to build a secure network. They all differ from each other, some a little, and some a lot. They often make you think and believe that you are 100 % dependable on them and their technologies! Now, what is interesting is, none of them can ever make your network 100 % secure!!! And why is that? Due to that fact that they don't know anything about your organization's business strategy, needs, routines, compliance and governance etc.

That's where you come in! You have the choice to be the network security catalyst! The passive "agent" which makes several compounds react, evolve and grow in a new strong and secure synergy!

Now you have a choice..!

I'll put 2 pills on your imaginary mind table, a blue and a red one. Either you take the blue pill or the red pill! Each pill contains a strategy. If you take the blue pill you quit reading the article and proceed with what ever you were doing! If you take the red pill… You keep reading, and you start seeing the actual framework, the actual grid, the network, for what it really is! And you start questioning it, rebuilding it, you start to innovate new strategies and a more flexible and robust framework around you and your organization, which leads to a more holistic, flexible and highly secure business driven network.

Good Choice!

Through the years, I have been privileged to work with many highly skilled and gifted people within computer science, administration, network administration, network design, network security and information security in general. I have worked and traveled in many countries, experienced a lot, I have been taught many interesting things and lessons on the road. When Hakin9 Security magazine contacted me and asked me if I wanted to write an article about network security I started thinking about which of my insights I wanted to pass forward. My inner observation through the years was, no matter how big or how small an organization is, without a clear understanding what is going on business wise you'll never be able to build a secure and flexible network, which supports measurable development and growth of the business you are working for!

Today many complex theories and strategies exist for what security is and how to apply it.

Some of them are very simple while others are highly complex and difficult to grasp and understand. One of my mantras is "keep things as simple as possible" This doesn't mean that technical solutions can't get complex, which they do in some cases. Remember that complex solutions demands much more resources such as technology and administrative overhead, which in many cases leads to lack of risk control, lack of oversight, lack of technical control etc. The list is long. I have been in many big companies which have spent millions of dollars on technology, without a clear intention, plan and strategy for how to think before they build. I often see that there is a lot of goodwill but so little strategy and awareness of deeper intentions behind design and implementation.

The CIA – Confidentiality Integrity Availability – triad model has existed for decades and is still one of the main principles and cornerstones within information security to this day. If you are not familiar with it I recommend you study it and use it in your daily way of thinking within the networking or security field. Many good frameworks of thinking are available like CISSP and SABSSA, but they take a lot of time and dedication to learn and implement! If you're not there yet, you can use a simple model I have been using for many years, which has been beneficial and proven successful in project after project. I call it "The Meta Network Security Strategy" and originate from a more holistic, cognitive and systemic way of thinking rather than only a best practice, business oriented or in a technical administrative way. "Meta" comes from the Greek term designating something that is above or beyond something else, it is above it at a higher level. Please note that this model is holistic and my own approach and invites the best information from different suitable systemic frameworks such as ISC CISSP® or SABSA Enterprise Security Architecture to be used! The advantage with a holistic approach is its' openness to systematic frameworks, where systematic framework doesn't leave room for holistic frameworks or thinking, simply because otherwise it wouldn't be systematic!

"The Meta Network Security Strategy"

- Step one – Intention
- Step two – Purpose
- Step three – Movement
- Step four – Resources
- Step five – Meaningful Actions

Intention

Why is intention important? Intentions are conscious or unconscious choices we make in our living, evolving as human beings. Working professionally for a living without intention, is meaningless and effortless. I believe that any kind of an organism has a deeper intention of surviving, growing and evolving in life, biological as well as business wise. For example; a business must earn money to survive and grow. So whatever job, project you are assigned to or whatever department you're sitting at, there is a clear intention behind why you are there and what you are working with, even though it isn't outspoken.

The challenge comes when you going to create something new or innovate old system designs or strategies. Even though you think you know how everything works, it is very crucial that you get the intention clearly defined and written down on paper! Ask questions, the more you ask the more you know, the more factual and nonfactual information you know the more of an expert you'll become!

Heisenberg said once,

"We have to remember that what we observe is not nature in itself, but nature exposed to our method of questioning."

Which means that the more you ask the more expert knowledge will you gain to solve the equation. The clearer intention, the more meaning your work will give you. My challenge has always been making all the intangible information and experimental knowledge into tangible abstract knowledge. The only way I have succeeded has been by asking questions! Well-educated leaders, business owners, CIO's 99% of the times show appreciation and interest in people who try to understand the organization and want to make a difference. Note! Assumptions, guessing, mind reading due to laziness are often causes to failure in strategy and design, which eventually end up with bad network security.

Well… Donald Trump stated once:

"You have to be insane about the details or the whole enterprise will fail."

Which I interpret as, if you are going to build something strong and solid, you need a clear intention and all the information you can get. The more information you get at this stage the easier it will be for you in the upcoming stages! See it as your questioning is making all intangible and abstract things you don't understand more tangible, precise, explicit, measured, concrete and empirical. When you have the full intention written down on paper, defined and all share the same perception of the intention you re ready for next step.

Purpose

Purpose is the key! Purpose gives meaning and goal directness. Without that there is no fundamental idea and a solid grounded process for where to go and from where. Purpose gives indicators, which make it possible to measure and benchmark processes. A process is defined by an intention driven purpose, where you start from A, actions is executed on the pathway and you end up at B.

Duglas W. Hubbard wrote;

"Humans possess a basic instinct to measure, yet this instinct is suppressed in an environment that emphasizes committees and consensus over making basic observations."

My own observation has been that many organizations are so thrilled over their own economical success and even more thrilled over a possible development or finding a technical security solution that they forget to observe, think, analyze observations and match the outcome with purpose and intention! Many lose their objective on their way to pursuing the real purpose, without knowing it! The reasons are often that companies either don't have leaders that understand security and why it is important or that leaders know that they should have security but don't want to pay for security, since it is an "insurance" anyway and finally the worse scenario a combination of both. It's very important that purpose is discussed, defined, written down in words so you have a loud and clear intention driven purpose, which support the business. This often means that it is aligned economically with the risk and possible loss of value if the worst case scenario should happen. When that is done you have a real opportunity to observe, measure and benchmark your security solution later on. Without the above, and let's say you are about to built a new secure network, how would you know where to start, how would you know to get the support you really need, from your directors, leaders you CIO, CSO or COO? Please note! When I write support, I don't mean money! I mean understanding from highest level of your organization and down to your level. Remember, money is only buying you short time help! While understanding, commitment and responsibility buys a lifetime of support! With out above how is it even possible to build a strong, well-thought and planned network security solution? It isn't…. and that is why we all have jobs today.

Movement

Movement is about going from somewhere to somewhere else! From A towards B. There is no rule that the path has to straight, curved or with stops on the way. From the higher meta-state of intention, which is a higher conscious level of thinking process, towards construct and development of a well-defined intention-driven purpose, which is at the lower level of the Meta-state thinking process. Movement is the part that you eventually end up no matter what you do. Movement is your chosen behavior, actions and responses, which must be seen as effective and valued due to your intention-driven purpose.

"Note everything that can be counted counts,
and not everything that count can be counted."
– William Bruce Cameron

My point here is that we most often do actions unconsciously, without thinking in depth about why, what intention or purpose it has. By thinking and making sure you have an intention driven purpose you ensure deep solid quality in your work and actions. Remember Solidity, Quality and Security goes most often hand in hand.

Furthermore it is your conscious, well-thought observations and actions that counts and not the technical framework, best practice or recommendations that you follow. I have seen many engineers blindly follow, best practices, recommendations and secure design solutions implemented without intention or purpose, which lead to security flaws and unnecessary economical expenses.

You have the choice to change the thinking process and alter the reality of true network security. Remember that you have a whole pallet of resources that you can use as tools on your way pursuing the intention driven purpose. Remember that it's not what you think or say in your process, it's what you do in conscious actions…! What ever you do in actions, it must support the defined intention-driven purpose.

Resources

What is a resource, where do they reside or exist and how do you facilitate them for the best possible outcome? All human beings have inner and outer resources, the most are not aware of them and use then unconsciously all the time, without a full potential, it may vary a lot, but I would guess that most people use from 50 to 70 percent of their full potential. Can you imagine what would happen if you became aware of all your resources and used them to their full potential!

Inner Resources

The inner resources are your inner way of thinking, all your experiences as human being, both as engineer and as person who interact with systems and other human beings, your profound technical knowledge, all of them, good as bad. They way you reflect up situations, the way you relate to past experiences and combine them with technical knowledge make you a huge and very strong knowledge bank. Remember. Knowledge and insight is the most pure form of power, and we all have it in different ways and degrees. Your inner resources will provide you a fantastic basis for decisions, thoughtful movements and actions related to any security design or solution that you want to implement.

As Morpheus said to Neo in the Matrix movie:

"I can only show you the door but you have to walk through it"

This is the exact same situation, don't think you have all resources, know you got it in you, and simply own it! Nobody can take it away from you. You learn and discover fast that the more you think, ask, propose and develop the more possibilities, thoughts and new ideas you'll get exposed to!

Outer Resources

Many outer resources are systemic resources in the form of systemic knowledge which many you already have encountered or know well. I assume that many of the readers already are certified network engineers, network security and/or information security. Many known frameworks exist today, educational such as Cisco cert. CCNA -> CCIE security, CEH, (ISC)^2 CISSP, CISM etc. to GRC framework such as PCI DSS, SOX, EURO SOX, HIPAA etc. All the systemic frameworks are well known and works well, and has been implemented millions of times all over the globe.

Unfortunately there is bliss and ignorance related to using these frameworks, which is that all frameworks are rigid, very steel and promise high security, which they are designed to for robustness and ease of logical access and understanding. This means that you one way or another are forced to compromise the optimal security design and solution due to following the specific framework. I have discovered that many engineers are often on unknown territory, and therefor they follow the frameworks and systemic thinking blindly without a plan of what the intention of the implementation is for in the long run. Often when I ask, why a network team or an engineer has implemented a security design or solution which don't fulfill it's purpose they answer, "Because the framework stated it was secure…"

The point here is that frameworks that are implemented with right intention works fantastic. Unfortunately, without a clear intention driven purpose or an intention at all it can become a catastrophe, money wise as well as support wise via administrative overhead and last and most often way to high technical complexity, which again lead to no control and bad quality and security.

Another outer resource is consultancy, which very often is systemic as well. Don't follow blindly, ask for intention and purpose and make sure that any proposal, design and solution really fulfill your intention driven purpose description. As a consultant myself, I have seen many poor security solutions implemented by consultants with no purpose of intention to fulfill, where I'm often tempted to think that it has been for the easy money and an easy fooled costumer.

Meaningful Actions

The last and fifth step is "meaningful actions". In "The Meta Network Security Strategy" meaningful actions is a positive outcome from previous described steps, which are:

```
Intention + Purpose + Movement + Resources =
Meaningful Actions
```

Meaningful actions are a solid holistic approach to understand the higher intention of the business while delivering high quality and high security with right purpose. Furthermore, since it is a holistic and a non-systemic model, it invites full systemic frameworks or just bits and pieces to be used and implemented for the exact specified intention driven purpose. The vice versa, such as a systemic model combined with a holistic approach, can never be done otherwise it wouldn't be systemic. The purpose of a system or framework is to deliver strict rules and boundaries for what can be allowed and not allowed. It's the simply the basic purpose of the system!

Another benefit of the system is every step towards last step is measurable. Measurability is one of the most important things in my personal work, because how do I know that I deliver a valued process, a positive difference and high quality, if I cant measure what I'm doing and the one I'm working for can't grade my job due to benchmarking.

So therefore when I work with costumers I always I always want to know where I'm at and what I'm want to accomplish through defined the intention and purpose of costumer. If I don't have these facts established I can't measure what difference I have made and I won't know if I have accomplished anything at all, besides spending time and money!

Conclusion

Customers exposed to the approach have been surprised over the power "The Meta Network Security Strategy" has, due to deep and strong fundamental work it provides. It gives a profound understanding and possibility for costume security design, integrations aligned with business needs without compromising any systemic frameworks which might be strict necessity due running the business. It's a strong process, which takes guts to pull though, but the outcome and transformation, is amazing in the long run. No quick fix, no superficial and useless designs that don't support you business in present sate and into the future.

I have met several who have challenged this process due to many of the systemic frameworks available, and they realized that "The Meta Network Security Strategy" is a way observing, seeing and reflecting security in the business, not a framework to follow. There are no rules, it can be used in thousands of individual ways and mark my words there is no right or wrong way to use "The Meta Network Security Strategy" there is only your way. Your mind is in your Matrix surrounding you! The more you dare the less boundaries exist in your path.

MADS BECKER JØRGENSEN

Mads Becker Jørgensen, 36 years old, Born and raised in Denmark, lives in Sweden. Mads works as "Security and Network Consultant" at Verizon Business and Terramark in Sweden, Mads works and has coaching workshops as Int. Cert. Meta Coach. In Mads's free time he is a Deep Ocean Free-diver and nature photographer, he is humble towards the world and his life, he love his life, family and friends. LinkedIn: www.linkedin.com/in/madsbeckerjoergensen.

Bugtraq "knock knock ...
Bugtraq has you ..."

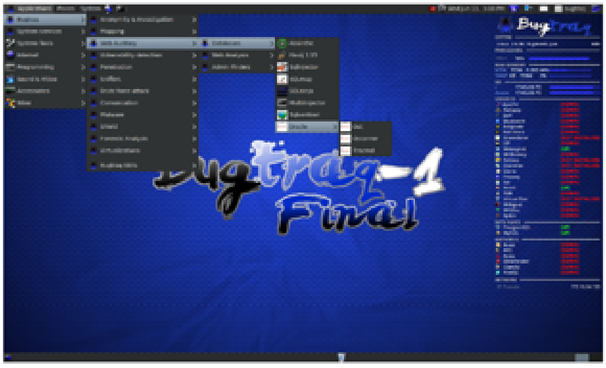
Feel the new revelation

The distribution known as Bugtraq-I, emerged from an independent project of two young enthusiastic Spanish guys. Noted for its easy use and easy configuration. Technically it is a stable and agile system in which applications are all automated and where the user can monitor all services of the system in real time.

Christian González and Rubén Galán creators of Bugtraq-1

Why choose Bugtraq-I?

There are multiple reasons, but the most notable one would be the global vision of the system that the user has with the conky interface. The friendly desktop makes an easy environment for a newbie user. Bugtraq-I is adaptable to any situation of ethical hacking.



Which applications/tools can you find in Bugtraq-I?

First of all, the majority of actual pentesting and forensic tools are incorporated in this system. These include tools of Windows that also work in Bugtraq. Next to that, you can find new branches of malware and anti-virus, with the purpose of empowering this unusual branch in GNU/Linux. Another type of tools are those that have been created by the Bugtraq-team. Lastly, Bugtraq-I also contains scripts for the installation of tools that require the user configuration, makimg a personal system in just a few minutes.

In which system is it based?

Bugtraq-I is based in Ubuntu 10.04 with the kernel 2.6.38 generic-pae. The dekstop environment is based in Gnome 2, optimized for the best performance.

What do you mean with automated applications?

One of the main differences between the actual pentesting distributions is that not a single unnecessary service runs in Bugtraq-I. Everything is thought through in such a way that the system intelligently selects the needed services to make the application work; like this the user monotorizes in real time all the daemons of the tools.

How to install?

You can download Bugtraq-I Final from official website. You can install it from a dvd or usb, where you have the option to use it liveCD or use the installer directly.

Are you planning to continue this project?

Yes, of course. We have created a private community in which we are developing new tools and giving the opportunity to grow to unknow or unsupported projects. The inscriptions have been closed on July, so if somebody want to participate, we will give 10 places for the readers of hackin9.

Internet Contact
Website: www.bugtraq-team.com **Twitter:** @BugtraqTeam
E-mail: staff@bugtraq-team.com
Pre-Inscriptions: inscriptionsh9@bugtraq-team.com

Enterprise Perimeter

Security On a Budget: Cisco PIX 500 Series Security Appliance

We hear about cutting edge technology being implemented by fortune 500 and 100 firms to protect their networks from unauthorized use. These solutions tend to be high end hardware and software solutions for high end security budgets. But many breaches tend to occur on smaller mid sized or small networks where IT Budgets are constrained well beyond the reach of that high end fancy IPS system."

What you will learn…

- How to secure your company's network on a budget
- How to operate with the CISCO PIX Security Appliance

What you should know…

- Basic knowledge of network security
- Basic knowledge of network equipment

As an independent network security consultant my client base can range from the small to mid sized firm to large fortune 100 firms. Routinely we hear about cutting edge technology being implemented by fortune 500 and 100 firms to protect their networks from unauthorized use. These solutions tend to be high end hardware and software solutions for high end security budgets. But many breaches tend to occur on smaller mid sized or small networks where IT Budgets are constrained well beyond the reach of that high end fancy IPS system. These networks make attractive targets to attackers for a variety of reasons and therefore also need to be protected with at least a reasonable level of defense.

Firms that have directly connected networks, particularly those hosting servers and web applications can be held liable for breaches of their networks that impact other firms. Unauthorized use can cripple smaller and mid sized firms that rely on electronic data to transact business. But affording both the high end equipment and personnel to maintain it can be unapproachable for many smaller and even mid sized firms. Let's face it, network security equipment usually isn't cheap. And these solutions usually don't end with cost of purchase. Cost of ownership can equal or exceed cost of purchase with higher end enterprise class solutions.

To save money many firms and small businesses often deal with local mom and pop shops which tend to push lower end small business tailored solutions that may or may not meet their needs. In some cases these solutions may work perfectly well and will provide a reasonable level of security based on assessed risk and performance requirements. But other firms find these scaled down small business versions may have limitations which are not a good fit for their overall requirements or preferences. Mid range firms often rely on SOHO solutions and end up sacrificing performance, reliability or features that an enterprise solution can offer. For these businesses there are still cost effective alternatives that can provide more features and often better security of an enterprise nature without an enterprise price. In this case I'm referring to previously owned and or refurbished equipment. The previously owned and refurbished Cisco and Juniper market is a growing and thriving industry and options abound both on public auctions site and actual authorized resellers in the refurbished market. But knowing what to buy, what constitutes a good buy and how to make it work for your network are key to utilizing these various options.

We'll look at some of this equipment and explore the possibilities and capabilities of deploying these solutions into the average small or mid sized firm where web facing services are offered in some form (SMTP\HTTP\HTTPS\FTP etc). For this article we'll be looking at one of my favorites for basic network security at the perimeter that provides enterprise class service and performance for a small to mid sized network budget, the Cisco PIX 500 series Firewall. The PIX is essentially a stateful inspection packet filtering firewall with some serious advanced layer features and capabilities built in It is not an application layer firewall (a feature boasted by the ASA via add on Modules) and is not intended to be the only layer of security protection for your web application servers but it can provide many application layer capabilities and can be integrated with application layer solutions to provide an overall network posture. As anyone reading this knows security involves multiple layers of protection that start on the wire and go all the way to the application. Today we're only going to be talking about the perimeter and basic defense for the network perimeter utilizing the Cisco PIX, an enterprise security appliance perimeter appliance from one of the worlds top network equipment manufacturers.

Cisco PIX 500 Series Security Appliance

As a consultant, I'm often put through the infamous "tech screens" by prospective firms prior to engagement of services. During this process I am often asked about the differences between the Cisco PIX Security Appliance and the ASA Adaptive Security Appliance. My usual response is to point out the ASA is built upon the same software foundation as the PIX, and utilizes the same commands and configurations as the PIX, and that without the add on Modules for application layer inspection the unit is essentially identical to the PIX, albeit better performing in some implementations and with some intrinsic advancements that make it an attractive purchase. On more than one occasion the person performing the screen has actually scoffed at this point and even gone so far as to tell me of some supposed new algorithm that is the adaptive security algorithm, never seeming to realize that the adaptive security algorithm is also utilized in the standard PIX 500 series Firewall (later referred to as "Security Appliance" which in fact it is given its additional functionality). This is a common misconception that hopefully we'll dispel herein.

The PIX IOS was built on a Unix based operating system called "Finesse" (Fast InterNET Server Executive) that was designed by Brantley Coile and John Mayes of Network Translation, Inc, and is now known as PIX IOS. The ASA runs "Security Appliance Code 7", which is built on the same PIX IOS software with some additional functionality built in. The commands are virtually identical. So is the interface of the graphical user interface used to configure and manage the device, referred to as the ASDM. Of course as is often the case in these types of screens I mentioned above, being right and the interviewer understanding you are right can be two different things. So sometimes I have to help them get there with regards to understanding the nature of the PIX and the ASA.

The fact is the PIX and the ASA are identical in most respects, which is no doubt why we see it deployed still in so many large corporate and government networks and why even though its reached "end of sale" it is still supported by Cisco TAC (and hopefully will continue to be supported beyond the proposed July 2013 date where it will reach "end of life"). The fact is Cisco made the PIX too good and other than replacing a fan or two over the years the PIX can prove to be a powerful perimeter edge stateful inspection appliance capable of some application layer filtering. In fact the PIX is capable of add on application layer capability when integrated with Websense which incorporates URL filtering giving it much more application layer functionality. So unless you're adding the additional security modules like the AIP-SSM for the ASA, then the ASA and the PIX are pretty much identical. Still if you have the money of course get the ASA. It's definitely a good purchase and you wont' be disappointed with a new Cisco ASA 5500 series appliance on your perimeter. But if not, ….read on.

PIX "EOS and EOL"

The Cisco PIX 500 series still retains much of its popularity as evidenced by both pricing on used equipment and the volume of selling and trading seen online. However the astute bargain hunter can find one for far less than paying for a new ASA. Again if you have the cash for a nice 5510 then buy all means it's a worthwhile investment. It's a great unit and offers some new features and the add on modules are well worth it. But there are specific reasons for buying the new ASA which in some cases may not necessarily translate to a direct benefit for your given network requirements. If your network budget is small (under $2000.00 for procurement and implementation) and you need a enterprise class perimeter edge firewall and maybe a few additional features (like site to site VPN) then the PIX still holds its own in the perimeter security appliance market and is still a viable option.

The PIX reached end of sale several years back however that doesn't necessarily translate to "end of life". The two are different states of support from Cisco. End of sale does not mean you cannot get support options for your PIX. In fact Cisco TAC still supports the Cisco PIX 500 series security appliance (with a valid Cisco Service Contract) and according to their website still will continue to do so up until July 2013. But even when Cisco TAC no longer supports the PIX until a non patched vulnerability is identified that cannot be mitigated then the PIX can still continue to prove a mainstay at any network perimeter that requires fast, efficient statefull inspection, 3rd Leg DMZ architecture and a wide variety of features including providing a terminating endpoint for DES3 IPSEC Client VPN's, IPSEC Point to Point Tunneling and even a limited number of application layer capabilities.

Which PIX to Pick

The PIX Security Appliance that fits the needs of most mid sized and small firms is the 515 or 515E. There are smaller models, more popular among smaller mom and pop shops that are often pushed to small and even in some cases mid sized business such the 506, 506E and the every popular 501. I never recommend these versions for the office unless you literally have less than 5 users and even then in some cases a 515 can often serve their purposes better and still save money depending on their usage and requirements. The first and most obvious drawback of these "SOHO" versions is the lack of a 3rd leg DMZ. The 515 includes an expansion slot for a 3rd leg DMZ or a 4 port DMZ card and the 501, 506 and 506E do not. The 520's are a good option if you can run with IOS version 6 as they are easily upgradable with the SE 440 BX motherboard, allowing you to add extra memory (regular DRAM) and a faster processor well beyond the original capacity for a faster more efficient unit. The drawback of the 520's however is you are capped at IOS 6.3, meaning no ASDM, no contexts or other advanced features that come with the new 7.x versions and above.

Concurrent connections are another stickler that can really create havoc in a small office where users frequent web searches and online web based applications. It is important to remember concurrent connections does not directly equate to the number of users. Cisco identifies concurrent connections as being based on a traffic mix of 80 percent TCP and 20 percent UDP with one host and one dynamic translation for every four connections (The concurrent connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections. – *http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/specs.pdf*). Basically that means socket connections (an IP address mapped to a layer 4 TCP Port) such as a web page being opened and the supporting UDP traffic (like recursive DNS queries). Multiple web pages opened by one user can utilize multiple existing concurrent connections causing page cannot be displayed messages for other users on smaller restricted models. But a fully loaded PIX 515 UR (unrestricted) avoids this for the average small and branch office requirement by providing up to half a million open concurrent connections. This is usually more than sufficient for offices of up to 100 users and therefore is the model of choice in most smaller or mid sized implementations.

Additionally performance measurements are going to show better throughput which will vary with load and utilization but will naturally be improved with a faster processor and increased memory. So again the 515 UR is the recommended model for the astute shopper in the previously owned market.

Hardening Your PIX

Understanding the PIX capability is essential to properly hardening it on your network. The good news is that out of the box the PIX is configured to block ingress traffic that did not originate from within the trusted network. So if your only use of your PIX is to provide a perimeter device to protect your internal clients then a few simple commands and you'll be online. There are still however ways to harden your PIX even with this straight forward configuration. And of course most users of the 515 have some sort of DMZ configuration that requires more steps to configure and harden the appliance and mitigate documented vulnerabilities. We'll examine a few of these vulnerabilities and ways on how to harden the PIX.

To DMZ or not to DMZ

Opening access through your PIX to web application resources such as web servers, mail servers, etc to the inside trusted network is easily doable via ACL's however this is not recommended. Bringing external web traffic into your internal trusted network opens the potential for transit attacks to internal trusted systems. Naturally isolating web application services from internal trusted hosts is the preferred method.

A standard 515 with a 1 port DMZ card will provide this functionality and allow you to utilize the less expensive "Restricted" model which limits concurrent connections and maxes out at a 1 leg DMZ. But if you want more interfaces for the 515 your next step up is the 4 port DMZ card but the card is not enough. You also will need to have the Unrestricted version of the PIX IOS to utilize over

3 interfaces on the appliance which is not difficult to find nor that much more expensive in the previously owned market. Both models however can be obtained at a discount and considering the only moving part is the fan longevity is usually not a factor. On a side note, I've never actually had a PIX just "burn out" on me. It's happened I'm sure, but not to me. And I've been configuring and working with the Cisco PIX since the mid 90s so that's a pretty long time to never have seen a "bad PIX". In fact I've even got half a dozen units from various release dates and they all work fine. I've just never seen one give up the ghost. So again my recommendation would always be get the 4 Port DMZ and UR bundle unless you have a very, very small office with very small office needs, in which case you likely wouldn't be talking to or paying for a network security consultant to design and secure your network perimeter. Keep in mind though once you start putting up corporate web apps scalability becomes a factor so having 3 extra DMZ ports for growth is worth the extra 100 bucks or so that it'll cost you to get the upgraded unit. My recommendation is always going to be to go for the UR bundle. It's worth the extra few bucks and you can add DMZ interfaces up to a total of 4 secured DMZ interfaces to build out your mission critical web application services.

Standard DMZ Architecture with the PIX 515 UR

The PIX DMZ assigns a security level to the DMZ that is between the no access "0" and all access "100". Standard settings would be 80 for the DMZ, 100 for inside and 0 for outside. Of course the number actually doesn't matter, as long as its between 0 and 100 it will not have access to the 100 (trusted) network and will still be accessible from the 0 (untrusted) network via an ACL. In the above diagram, the outside interface (Security level 0) sits at 10.1.1.1/28 (using an RFC 1918 address for the purposes of this article, normally this would be a registered IANA address). The inside trusted interface of the PIX (Security level 100) sits at 172.16.10.1/24 and brings established traffic (traffic that originated on the inside) as well as trusted IPSEC client VPN traffic to the inside trusted network (Figure 1).

Outside web clients needing access to a proprietary database on the inside trusted network establish encrypted DES3 sessions with the outside interface of the PIX and are then able to access a proprietary database application on the inside network. The VPN uses the Cisco Secure VPN client or you can also use other 3rd party VPN client software on your client computer, such as NCP Secure VPN Client or Shrewsoft. I've found the NCP Secure Client works well with the PIX when for newer 64 Bit Client VPN access. Additionally it provides a good client for the MAC OS. Unfortunately Cisco's standard VPN Client does not run on 64 bit architecture.

For ease of use you can simply create VPN "Group" accounts on the PIX to mimic user accounts forgoing the need for additional equipment or software so if you really want to go on the cheap

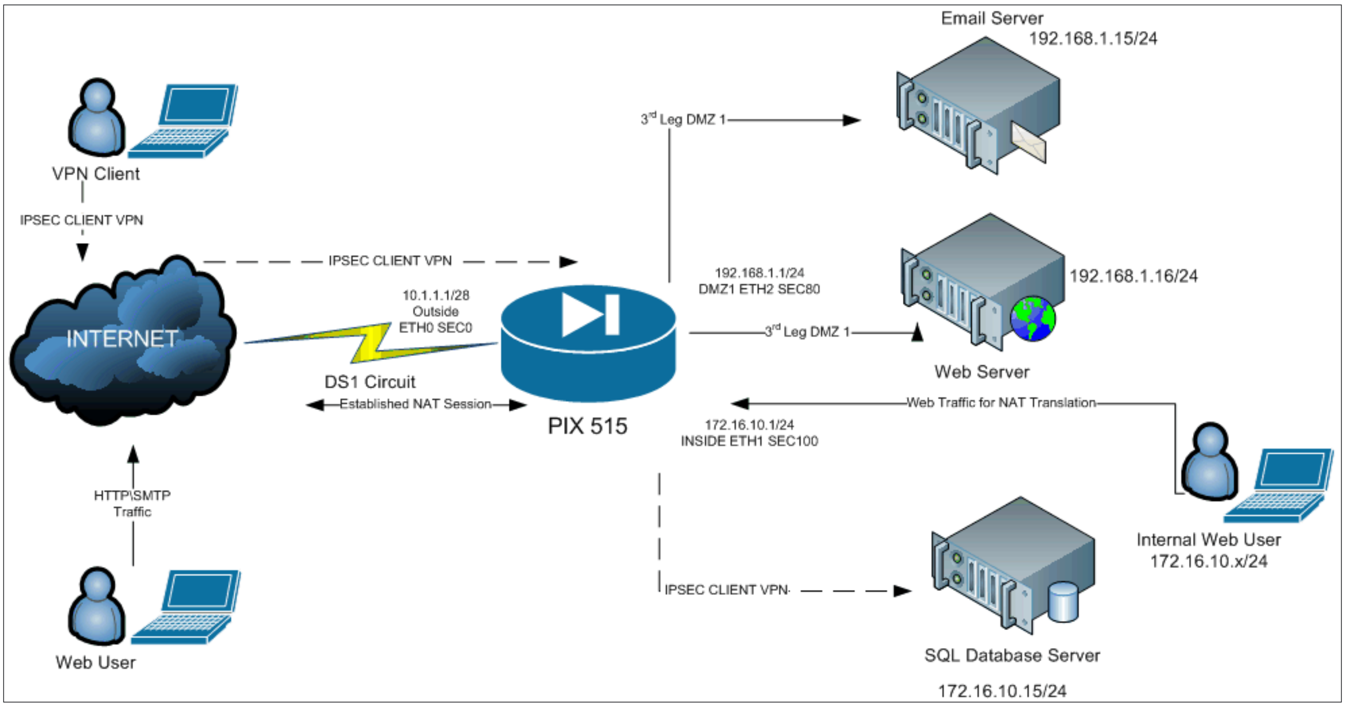


Figure 1. *Standard PIX Deployment with 3rd Leg DMZ*

and use no third party authentication you can literally use the PIX as your only VPN client endpoint, although I don't advise it in most instances. Personally I prefer not to have my firewall also be responsible for terminating VPN client sessions on the external interface and given that there are other options out there that too are cost effective for configuring a lateral VPN solution I usually recommend a dedicated VPN appliance sitting adjacent to your perimeter device. But enough for now on the VPN functions of the PIX. Perhaps down the road in a later article we can address that but for now we'll leave the VPN capabilities for another time where space and time permit.

Back to the above diagram you can see that unencrypted anonymous HTTP web traffic as well as SMTP traffic is being diverted via a 3rd leg DMZ to the mail and web servers which are securely isolated from the inside trusted network. This traffic is firewalled at the DMZ and not permitted to traverse the PIX into the trusted internal network. This is a pretty standard and straight forward deployment but gives you a general picture of a typical branch office deployment where web application services are being offered to the general public.

Configuring the PIX

Basic commands to get the PIX online are fairly straight forward. Following are some basic commands that are just enough to get the box up and running and allow clients to access your web application servers. In this instance open traffic to a standard SMTP server (running on TCP 25) is being permitted. FIXUP protocols or "inspect" is assumed. These commands were performed on a Cisco PIX 515 UR running Cisco PIX IOS 8.0(4).

- `PIXFIREWALL(config) # interface Ethernet0` (enters interface configuration mode)
- `PIXFIREWALL(config) # nameif outside` (names the outside interface and brings it up)
- `PIXFIREWALL(config) # security-level 0` (sets the security level, this is the default, 0 means no ingress access unless permitted)
- `PIXFIREWALL(config) # ip address 10.1.1.1 255.255.255.248` (set outside IP address)
- `PIXFIREWALL(config) # interface Ethernet1` (enters interface configuration mode)
- `PIXFIREWALL(config) # nameif inside` (names the inside interface and brings it up)
- `PIXFIREWALL(config) # security-level 100` (sets the security level, this is the default, 100 means all egress access permitted)
- `PIXFIREWALL(config) # ip address 172.16.10.1 255.255.255.0` (set internal IP address)
- `PIXFIREWALL(config) # interface Ethernet2` (enters interface configuration mode)
- `PIXFIREWALL(config) # nameif DMZ1` (names the DMZ interface and brings it up)
- `PIXFIREWALL(config) # security-level 80` (sets the security level to a midway point between the external untrusted network and internal trusted network)
- `PIXFIREWALL(config) # ip address 192.168.1.1 255.255.255.0` (sets the address of the DMZ interface)
- `PIXFIREWALL(config) # global (outside) 10 1.1.3.-10.1.1.4` (creates a NAT pool of IP's for internal hosts to use to access the outside, normally these will be registered IANA addresses, however for the purpose of this article we're using RFC 1918 addresses)
- `PIXFIREWALL(config) # global (outside) 1 interface` (sets the outside address of to be used as a PAT address once addresses from the NAT pool are exhausted. Since we're using a small external subnet only 2 free mappings are available and then the PIX will roll egress traffic over to PAT utilizing the 10.1.1.1 address of the external interface)
- `PIXFIREWALL(config) # nat (inside) 1 0 0` (enables NAT for the entire internal subnet)
- `PIXFIREWALL(config) # nat (DMZ1) 1 0 0` (enables NAT for the entire DMZ)
- `PIXFIREWALL(config) # static (DMZ1,outside) 10.1.1.5 192.168.1.15 netmask 255.255.255.255` (map a static IP to the internal IP of the mail server sitting on the DMZ, note the 32 bit mask identifying the host, and not the actual subnet mask of the wire)
- `PIXFIREWALL(config) # route outside 0 0 10.1.1.2` (sets the default gateway of the PIX to the next hop, normally this will be your ISP)
- `PIXFIREWALL(config) # access-list 101 extended permit tcp any host 10.1.1.106 eq smtp` (permit mail traffic to the mail server on the DMZ from any host. SMTP denotes TCP port 25 however if your server uses a different port simply insert the port number rather than the protocol id)
- `PIXFIREWALL(config) # access-group 101 in interface outside` (apply the ACL to the outside interface)

As you can see the basic commands are pretty straight forward. NAT\PAT, ACL's, security levels to set trusted and untrusted status and interface configuration mode similar to a regular router and of course basic route commands. But this is just the tip of the iceberg. Many more options, features and commands are available and we'll briefly take a look at just a few of these.

Hardening PIX IOS: Vulnerabilities and Versions

There are plenty of additional ways to help harden the PIX depending on your implementation, requirements, etc. There isn't the space herein to cover these commands in detail. The PIX has a wide variety of features, capabilities and configurations which is what makes it such a dynamic security appliance, but we'll briefly highlight a few that can be helpful.

Vulnerabilities

This is where a lot of misinformation about the Cisco PIX usually enters the picture. Often network administrators and engineer's base decisions on partial information with regards to the PIX and rumors about vulnerabilities, end of life, etc can dissuade some from choosing the PIX as a platform. But in reality the PIX is still a viable option and holds its own as a network security perimeter appliance. The version of the PIX IOS you want to run does depend on platform. Its not uncommon to see PIX 520 series firewalls still installed in some older networks and 506, 506E and 501's which are common on smaller SOHO networks. These models are limited on the version of the PIX IOS it will run. The newer versions (7.x, 8.x) will not run on these models and hence will not run the ASDM. So if you're fine with old 6.x PIX IOS and straight command line (don't say PDM, PDM bad, very bad…) then these are fine. But it's always best to run the latest greatest and given the 7.x and 8.x versions can host the same Cisco ASDM that comes with the new ASA Adaptive Security Appliance you'll normally want to go with the 515 series. The 515's run IOS 7.x and 8.x and give you the full ASDM just like the ASA's (Cisco's new feature rich highly functional graphical user interface for the PIX\ ASA) and also runs "contexts" which basically lets you be your own ISP by permitting multiple isolated subnets on a single external interface. You can have multiple circuits terminating into single PIX which is good for providers of service or even redundant connections.

The primary reason for concerns about PIX IOS version is of course reported vulnerabilities in a given version. A lot of anecdotal accounts abound in network teams about vulnerabilities in the Cisco PIX and often I hear engineers claiming you need an ASA because the PIX has documented vulnerabilities. But this is again a common misconception. The fact is the basic PIX IOS platform is the same one being offered on the ASA therefore these vulnerabilities in question usually will either impact both devices or not impact both devices. The good news is these vulnerabilities are not necessarily as severe as some think and others claim. In fact in most cases they won't even impact your implementation and often aren't even applicable, depending on the version of the IOS you are running on your model and your given network architecture, requirements and usage. We'll look at a few of those vulnerabilities, how they can be resolved, mitigated or worked around and whether or not they even apply to your particular implementation.

TCP State Manipulation Denial of Service

Perhaps the highest profile vulnerability in the Cisco PIX is the TCP State Manipulation Denial of Service vulnerability. This is a simple vulnerability and not necessarily a hack but simply a way to employ a denial of service (DOS) attack against a PIX guarding a perimeter. TCP State Manipu-

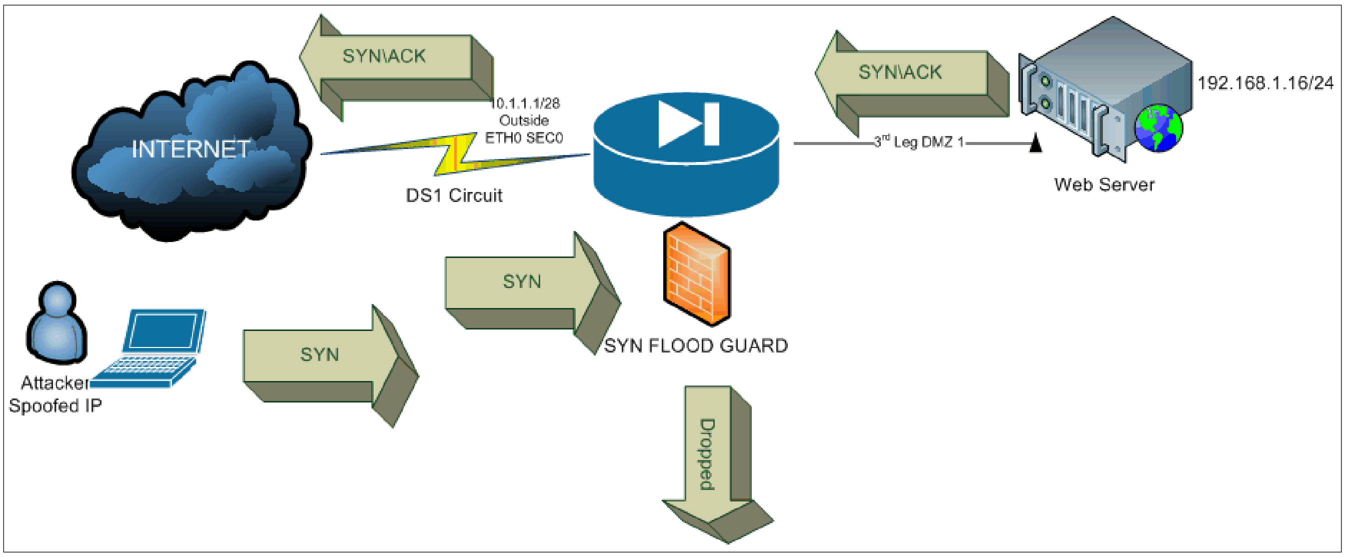


Figure 2. *Basic SYN Flood*

lation is similar to the old “half-open SYN” technique in that unacknowledged packets can be left in an infinite state, in most cases “FIN_WAIT1”. Open enough connections and leave them in a hung state and you can block connections to the device (Figure 2).

However in this case Cisco states the attacker needs to first establish a TCP 3 way handshake which of course is different from a half-open SYN since with a half-open SYN the 3 way handshake never completes by design.

Cisco patched this issue a long time back, as early as one of the 7.x releases. The following versions of respective releases however have been patched.

- 7.1 (2.79)
- 7.2 (4.18)
- 8.0 (4.9)
- 8.1 (2.3)

Additionally the issue can be somewhat mitigated on affected versions by limiting the timeout on connections. The shortest timeout is 5 minutes and can be implemented using the following command.

```
PIXFIREWALL(config) # timeout half-closed 0:5:0
```

Of course mitigation is quantified by risk and requirements so best bet is to either buy your PIX with one of the IOS versions referenced above pre installed or take steps to upgrade your unit to a version unaffected. SYN Flooding is now handled by the “Static” NAT command and half open SYN connections where an attacker uses a spoofed IP address to initiate a SYN handshake with a system protected by the PIX are protected when a static NAT mapping is enabled assuming you specify the max open connections a max embryonic connections in the command line. You’ve probably seen a line similar to this before.

```
PIXFIREWALL(config) # static (DMZ1,outside)
10.100.1.16 192.168.1.16 netmask 255.255.255.255 0 0
```

The last two zeros at the end indicate the max open connections and max embryonic connections. `0` means unlimited, so this system is not protected. To correct this you’ll need to set the max open connection and embryonic connection value.

Using the “show local host command you can see the current connections against the limits you defined. In this instance no limits were defined since the default “0” is set.

```
PIX# sh local-host
Interface DMZ: 0 active, 0 maximum active, 0 denied
Interface inside: 8 active, 18 maximum active, 0
                 denied
local host: <192.168.1.16>,
    TCP flow count/limit = 0/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 1/unlimited

  Xlate:
    Global 10.1.1.16(12407) Local
                 192.168.1.16(36541)
```

Setting the values for max connections and max embryonic connections limits these connections on to the local IP and drops those beyond the established parameters. The first value is maximum connections, the second is maximum embryonic connections. This command is issued the same in both PIX IOS 6.3 and 7.x +.

```
PIXFIREWALL(config) # static (DMZ1,outside)
10.100.1.16 192.168.1.16 netmask 255.255.255.255
                 2500 2000
```

This instance limits maximum connections to 2500 and maximum embryonic connections to 2000. Additionally you can protect NAT connections on the inside using the same method.

```
PIXFIREWALL(config) # nat (inside) 1 0.0.0.0
                 0.0.0.0 5000 5000
```

This instance limits both max connections and max embryonic connections to 5000 each. Of course these are just examples and would need to be tailored to your own individual requirements. Keep in mind, a single user will use many connections so don’t set this value based solely on users but on usage.

Enhanced Inspection of Malformed HTTP Traffic

One of the higher profile vulnerabilities in the Cisco PIX IOS is the enhanced inspection of malformed HTTP traffic vulnerability which refers to the enhanced HTTP inspection feature of the Cisco PIX IOS. The issue is malformed HTTP packets can cause the appliance to crash. Regular HTTP inspection however is not affected, so unless you manually set an HTTP inspection map then your appliance is not vulnerable.

In addition, the following releases of the IOS have been patched. Appliances running the following versions have been patched and are not affected.

- 7.0(4.14)
- 7.0(5)
- 7.1(2.1)
- 7.2(1)
- Later releases not affected

Inspection of a stream of malformed TCP Packets

Again the system can be caused to hang by sending a stream of malformed TCP packets either to or through the device. And again there is a work around and patched versions that mitigate and altogether remove the vulnerability. The work around is to limit the maximum TCP segment size. One simple command accomplishes that.

```
PIXFIREWALL(config) # sysopt connection tcpmss
                         minimum 64
```

Additionally units with the following PIX IOS release are not affected by the vulnerability.

- 7.2(4.18)
- 8.0(4.9)
- 8.1 (2.3)

Release 8.2 and beyond are not affected.

These are some of the more high profile and recent vulnerabilities and obviously we can't take the time here to document every vulnerability in the PIX IOS over the years. But this provides a decent overview of the more prominent issues and how they can be mitigated and or resolved. Work arounds and patches do exist for the PIX and so its important not to let rumor or misinformation deter you from implementing a PIX to protect your network perimeter and provide fast, efficient ingress and egress traffic flow, NAT\PAT and other gateway features. The PIX is still a viable option for businesses and other entities looking to secure their network perimeter but that don't have the budget for a newer more expensive model.

Syslogging

Syslogging is nothing new and anyone reading this article is likely well acquainted with syslog servers so I wont' spend a lot of time here. The PIX by default does not send syslog messages so you'll need to turn it on and point it to the syslog server on your network. Syslogging is an inexpensive way to monitor activity on your firewall appliance and network so I strongly advise setting one up with your PIX. Cisco made a fantastic little syslog server (pfss.exe) but I don't think they offer it these days. It used to be a download from the CCO website that you could download with a CCO login. Pfss.exe is a simple text based syslogger that runs over standard UDP 514 and creates text files for each days logging, dividing up logs by the day of the week. When a week completes pfss.exe automatically creates a subdirectory in the syslog folder and starts a new series of daily text files, each named for the respective day of the week its logging. There's plenty of good sysloggers out there of course, many with parsing features well beyond a simple text logger. But on a budget you'll find pfss.exe to be a great free option, assuming you can find it.

Setting up logging on the PIX is pretty straight forward. There are several options you can set but these three are really all you need to enable syslog on the PIX. First use the "logging enable" command and point it towards your syslog server and the interface it sits on. Following is an example assuming your logging server sits on 10.1.1.110.

- `PIXFIREWALL(config) # logging enable` (turns on logging)
- PIXFIREWALL(config) # logging trap informational (sets the level of information in logging messages, settings are between 1-7 and can be numbers or named)
- `PIXFIREWALL(config) # logging host dmz 10.1.1.110` (points the syslog messages to the logging server in this instance sitting on the DMZ over UDP port 514)

There are other options and settings however just to get basic syslogging up and running. You can also send logging to the ASDM for a nice graphic interface to review real time syslog messages.

```
PIXFIREWALL(config) # logging asdm informational
```

Threat Detection

Basic threat detection on the PIX is enabled by default in the IOS. Basic threat detection can detect various sorts of attacks, usually based on dropped packets over a given, preset time sampling. This sampling however can be modified for identifying and targeting specific incidents or hosts in an ACL for example, and include a basic and burst rate value.

Fragmentation Guard

Fragmentation guard is a feature of the PIX IOS that helps protect against common fragmentation attacks like “Land”, Teardrop” and other forms of network attacks that utilize fragmentation. Use of the fragguard feature includes utilizing syslog reporting. You’ll want to have your syslog server set up to fully utilize this feature. To implement fragguard on your PIX using pre IOS 7 use the “sysopt” (“sysopt” is a command used by the PIX to define exceptions capable of bypassing the adaptive security algorithm and access control lists. Common uses include exceptions in IPSEC tunneling and L2TP) command.

```
PIXFIREWALL(config) # sysopt security fragguard
                (pre-IOS 7)
PIXFIREWALL(config) # fragment (post IOS 7)
```

With PIX IOS 7 the sysopt security fragguard command has been replaced with the “fragment” command. The fragment command permits full packet reassembly as well as fragment size parameters and more. Combined with a syslog server you can use this feature to identify and help prevent attacks like Teardrop. Parsing your syslog server messages for “106020” will help identify Teardrop attacks. This is a common entry in a syslog message identifying Teardrop.

```
%PIX-2-106020: Deny IP teardrop fragment
```

Additional parameters in the message include the “size”, “offset” and the all important source and destination IP address making it easier to identify the attacking host.

AAA Floodguard

Floodguard is a standard feature on the PIX that protects against too many open authentication requests when using AAA Authentication and is actually enabled by default. Floodguard clears out AAA request connections in order as the system is bogged down in the following order.

- TIMEWAIT
- FINWAIT
- Embryonic connections
- Idle (Figure 3)

Floodguard is enabled or disabled with the following command in PIX IOS 6.3,

```
PIXFIREWALL(config) # floodguard enable
```

In Version 7 no command is needed as AAA floodguard is always enabled.

Mailguard

Mailguard is an advanced feature on the PIX which limits SMTP commands to the PIX to limit attack options to your mail server. Mailguard is pretty straight forward when it comes to protecting your SMTP server by limiting the available commands permitted to it through the PIX to seven basic RFC 821 (As outlined in RFC 821 section 4.5.1) commands, HELO, RCPT, MAIL, DATA, RSET, NOOP, and QUIT and not permitting more vulnerable commands like “KILL”. Mailguard is enabled by default on later versions (post IOS 5.x) of the PIX IOS via the `fixup protocol smtp 25` command (Figure 4).

In 7.x the `fixup` command has been replaced with the `inspect` command. In some cases this can cause issues with mail servers like some versions and implementations of Exchange so disabling this feature in some instances can be necessary, however with

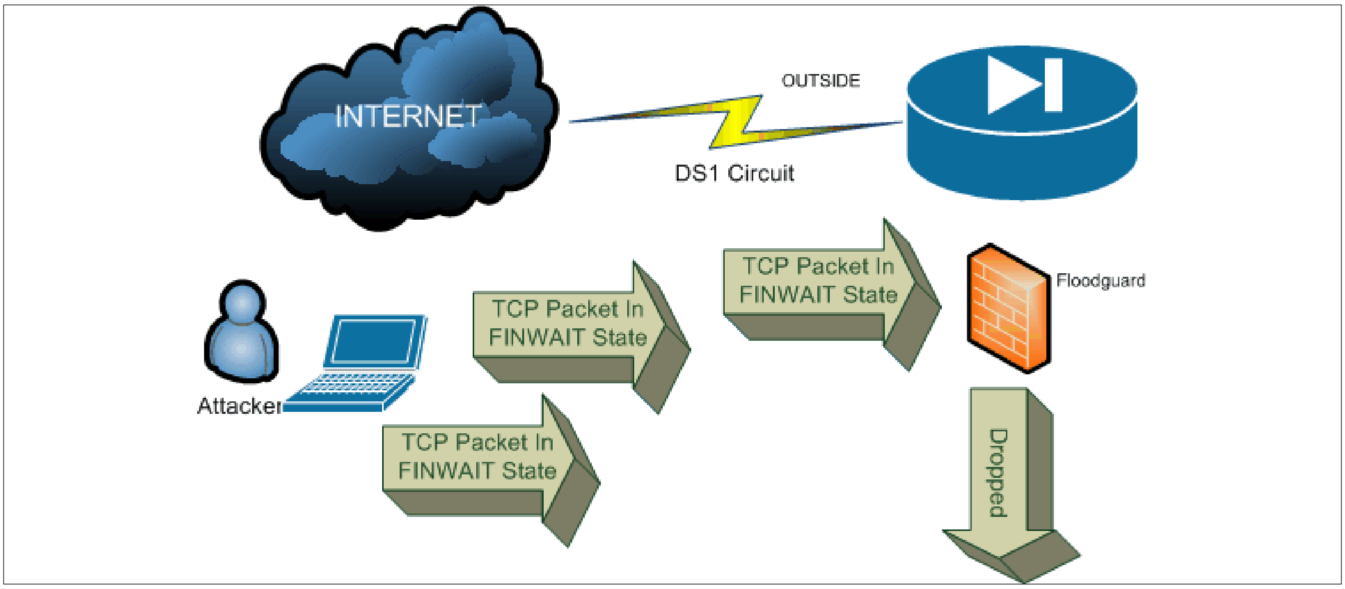

INTERNET
OUTSIDE
DS1 Circuit
TCP Packet In FINWAIT State
TCP Packet In FINWAIT State
TCP Packet In FINWAIT State
Attacker
Floodguard
Dropped

Figure 3. *AAA Floodguard*

later versions of Exchange its normally not an issue. I personally leave Mailguard enabled routinely in front of Exchange 2010 with no issue due to the way later versions of Exchange handle opening communication requests like EHELO. If you want to know if Mailguard is enabled behind a PIX an easy way to test is to simply telnet via TCP 25 to the server. If you see the following then Mailguard is enabled.

```
220**************************0*2******0***********
2002*******2***0*00
```

To enable Mailguard use the following commands;

```
PIXFIREWALL(config) # fixup protocol smtp 25 (pre
                PIX IOS 7.x)
PIXFIREWALL(config) # inspect esmtp (post PIX IOS 7.x)
```

Unicast Reverse Path Forwarding

Unicast reverse path forwarding is a feature on the PIX that helps reduce the risk of IP spoofing by verifying the path of a packet traversing the PIX. The command is interface specific.

To enable unicast reverse path forwarding on the outside interface of the PIX use the ip verify reverse-path command.

```
PIXFIREWALL(config) # ip verify reverse-path
                interface outside
PIXFIREWALL(config) # “show ip verify statistics”
   (displays statistics on dropped RPF packets)
```

URL Filtering

Unlike the Netscreen, URL filtering is only possible with use of an external Websense server so we won’t spend time on this option other than to show a basic command example should you have access to a Websense server.

```
PIXFIREWALL(config) # url-server (dmz) vendor
websense host 10.1.1.110 timeout 15 protocol TCP
                version 4
```

This article contains just a high level overview of some of the features and capabilities of the PIX. Again neither time nor space permits a thorough examination of all the various features, capabilities, commands and configurations possible on the PIX. That would take a book (of which there are some good ones out there). But hopefully this gives those considering the PIX a good snapshot of some of the more prominent features, functions and capabilities and what to look for when buying one.

Buying a previously owned PIX Firewall

There are many Cisco resellers out there and it’s not difficult to find one so this article won’t even begin to try to provide any sort of list of resellers and refurbishers. Ebay of course tends to be a favorite these days simply because of the low prices, such as getting a nice new 515UR for 75 bucks (its been done, believe me) but more often the usual price for a 515UR with 4 DMZ ports is around $300 dollars, give or take. That’s from a confirmed seller with a good track record and of course a print out of the basic show ver and show run to show you the system’s up and working. But it ranges in price depending on the version of the OS, the condition its in, the seller, the number of DMZ ports (1 or 4),

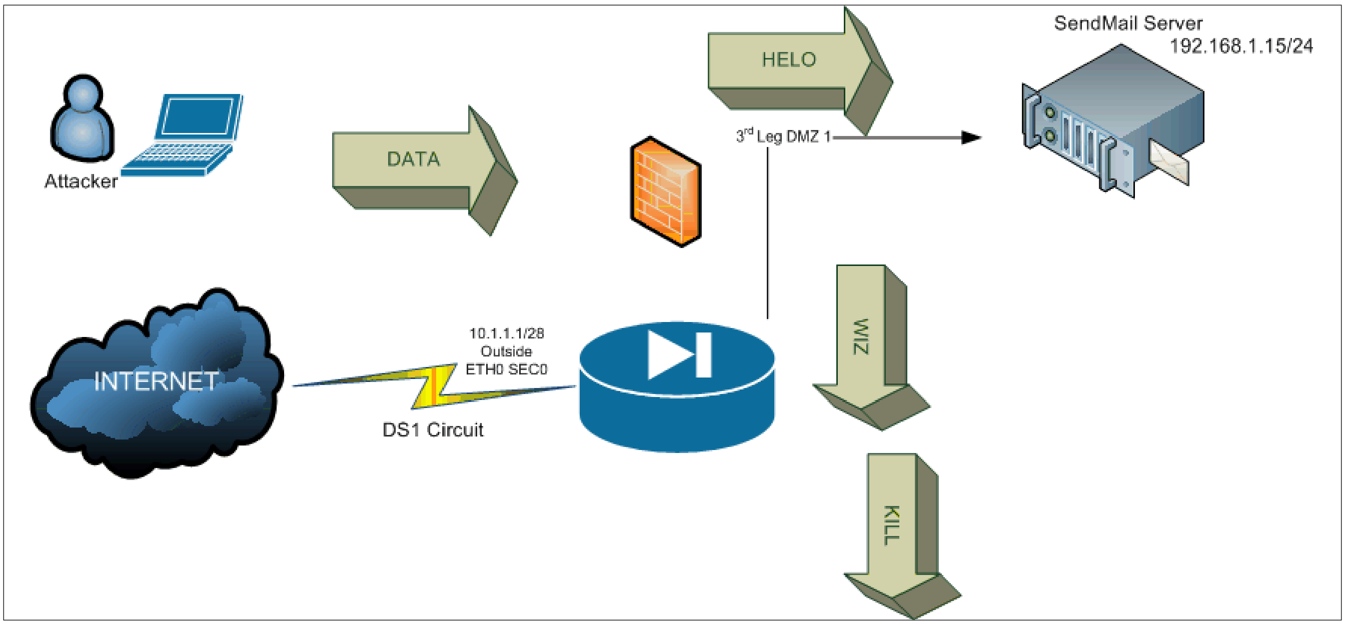


Figure 4. *Mailguard*

etc. Right now as of this writing I see them as high as $1500.00 and as low as $169.00 (UR, version 8.x IOS and 1 port DMZ for $169.00, great deal). So the astute shopper is probably going to find the best price on ebay however that's not always the case. And if you need a CCO Service Contract a reseller is going to be better able to provide that, something you probably won't find on eBay. But if you know how to configure it yourself or have someone in your organization who can and assuming you purchase one with the version of the PIX IOS you want then eBay can provide a great option for purchasing a previously owned unit or even a new one (old stock, new unopened unit) and I've purchased many a unit on eBay and to date have never gotten a bad or non functioning unit doing so. But I've also purchased from the wide array of excellent refurbisher's and previously owned product vendors with equally satisfied results so the choice is entirely up to you. For warranty and TAC support, the reseller might be the better way to go if this is your first purchase.

In Closing

I hate to stress this too much but again, please bear in mind this article cannot begin to cover the wide array of commands, configurations and options for the Cisco PIX Security Appliance and does not attempt to. There is so very much I wanted to cover but space and time just does not permit. There are multiple capabilities not covered including features like Failover, IPSEC tunneling or using a PIX as a client VPN endpoint (a powerful feature that turns your PIX into a VPN appliance without the use of a VAC card). Nor did we cover using the PIX in "transparent" mode which effectively bridges traffic through the PIX at Layer 2. Unfortunately neither time nor space would permit for such an in-depth review in this one short article. A review of PIX VPN capabilities, configurations, etc would require an entire article in and of itself as could transparent implementations, tunneling, etc. But hopefully if you are considering a purchase of a perimeter based security appliance this will give you a good overview of the benefits and features of the Cisco PIX Firewall and some tips on what to look for and on procuring one in some of the previously owned markets.

Also its important to remember the PIX is not intended to be the only component of security for your network. I cannot state that enough. A Stateful Inspection perimeter device is just one tier of network security and is not intended to be a catch all for your firm's web based applications. Application layer filtering, code hardening, pen testing, audits, etc are going to all factor into security for web application services and Hakin9 Magazine is chocked full of valuable information in these areas and can be a great resource for you in addressing the wide array of defense steps needed to secure the network and your web application services. But combined with a proper security policy and architecture, periodic testing and other steps based upon your assessed risk and requirements the PIX 500 Series Appliance still provides enterprise class perimeter access and security that goes much further than standard stateful inspection for businesses both mid sized and small when SOHO solutions are not enough and budget constraints are potential barriers to security. The PIX is still a viable candidate and given its end of sale status a bargain to boot. So if you fancy yourself a bargain hunter and need enterprise class security for your small to mid sized network and a SOHO solution doesn't fit the bill the PIX still offers enterprise class security and performance and now is procurable without the enterprise class price tag.

On the Web

http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/specs.pdf – The concurrent connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Glossary

`Sysopt` is a command used by the PIX to define exceptions capable of bypassing the adaptive security algorithm and access control lists. Common uses include exceptions in IPSEC tunneling and L2TP.

CHRIS WEBER

Chris Weber is a freelance Network Security Consultant with more than 15 years in the field of network security, analysis and design and has consulted on network security issues and incident response for multiple commercial organizations including fortune 500 and fortune 100 firms as well as US Federal Government organizations. Mr. Weber has held multiple industry certifications throughout his career including Cisco, Microsoft and others, and is currently an authorized Juniper Consulting Partner. Currently Mr. Weber consults via his own freelance consulting firm "Layer 9" located in Northern Virginia and can be reached at cw@layer9security.com.

HACKTIVITY

The IT Security Festival in Central and Eastern Europe

October 12-13, 2012. MOM Cultural Center, Budapest

THE LARGEST IT SECURITY FESTIVAL IN CENTRAL AND EASTERN EUROPE WILL BE HELD AGAIN! Real festival mood, peresentations, workshops, games, hardware hacking, lockpicking, big friday party and 1000+ hackers from all over the world!!!

Keynote Speaker:

Jeff Bardin, USA

Jeff is the Chief Intelligence Officer for Treadstone 71. In 2007, he was awarded the RSA Conference award for Excellence in the Field of Security Practices. He is the most respected expert in the field of cyber crime, cyber terrorism, cyber inteligence.
This talk covers the cyber intelligence lifecycle including examples of denial and deception. Open source intelligence (OSINT) is a critical aspect of asymmetric cyber warfare. It is part of the mosaic defense and one practiced as a method of unrestricted warfare. Methods of cyber espionage, sock puppet creation, infiltration, data collection and analysis are covered. Case studies on creating your own personas while using OSINT tools will be discussed.

...and who can you look forward to?

ZOLTÁN BALÁZS / HUNGARY --- Zombie browsers, spiced with rootkit extensions
ALEXANDER POLJAKOV / RUSSIA --- Top 10 SAP vulnerabilities and attacks
JOE MCCRAY / USA --- The Evolution of Pentesting High Security Environments
ANDRÁS KABAI / HUNGARY --- Hunting and exploiting bugs in kernel drivers
ALEXANDER KORNBRUST / GERMANY --- Self Defending Database
VIVEK RAMACHANDRAN / INDIA --- Malicious Wi-Fi Routers for Fun and Profit
MIROSLAV STAMPAR / CROATIA --- Spot the Web Vulnerability
BOLDIZSÁR BENCSÁTH / HUNGARY --- Duqu, Flame, Gauss malware analysis experiences
SHAY CHEN / ISRAEL --- Diviner the new OWASP ZAP extension

PAYPASS VULNERABILITIES **HSRP INSECURITIES** **„CHIP-TWEET"** **TRACING MOBILE PHONES**
ALTERNATIVE USAGE OF PKI DEVICES **LOCKPICKING 2.0** **ALTERNATIVE INTERNET**
USB = UNIVERSAL SECURITY BUG **iOS SECURITY** **ANDROID SECURITY** **NAT ATTACK**
BROWSER BASED ATTACKS **DIGIPASS INSTRUMENTATION** **SECURITY CODE REVIEW**
GEEK GIRLS **ELITE SOCIAL NETWORKS CROOKS** **AV INSECURITIES**

AND WHAT ELSE?!

Hello Workshops. Jump from theory to practice: **Hello Injection** **Hello CA** **Hello Code Review**
Hardware hacking / Lockpicking (non-destructivelock-opening) workshop and Urban Warrior competition / **24 hours - Hacker road reloaded.** Get prepared. Never experienced any similar game. Form a team, with a good hacker, a good lockpicker, a good social engineer.

Tickets are available until 20th of September with 10% discount on www.hacktivity.com

Full price for adults: 68 EUR / for companies: 150 EUR / Cheap hotels offering also there!

Special packages:

2 days ticket & 2 nights in a hotel***	199 EUR
2 days ticket & 2 nights in a hotel****	299 EUR

packages.hacktivity.com

Sponsors:

Further information and registration: www.hacktivity.com

Deloitte. rrc THINK VALUE. biztributor WEBSHARK ARUBA networks AdNovum FORTINET Hakin9 All About IT Security asc

Unified Threat

Management (UTM) – Save Time, Save Money, Secure the Network

In years gone by Unified Threat Management (UTM) appliances and services from vendors in the security industry have been led by the firewalling industry leaders who simply bolt on OEM versions of web filtering, gateway anti-virus, mail filtering and IPS.

What you will learn…

- Why UTM legacy vendors are behind the times.
- How to centrally manage the security estate.
- What is meant by true UTM.

What you should know…

- An understanding of security related services such as anti-virus, web filtering, spam filtering and firewalling
- Who the general players are in the security industry
- What UTM is

In the last few years there has been a buck in the trend whereby vendors in other market sectors of security are bringing "true" UTM solutions to the market space.

Unified Threat Management (UTM)

Unified Threat Management or UTM is the use of a single device within the network to secure the entire infrastructure via a single, hardened, vendor's gateway solution.

For many years there have been two main patterns to securing the IT network. Either a path of multi-vendor/multi-tier securing or single-vendor Unified Threat Management (UTM).

Multi-vendor/multi-tier security has been, for many years, the best methodology of securing the network. The reason for this is that multiple layers of security from multiple vendors gave the appearance of a higher level of security. This was based on the signature releases from multiple vendors being released at different times and therefore, hopefully, catching that illusive zero day attack.

With a multi-vendor approach, the level of security is of a high standard, however, the cost for administration and maintenance of patch levels, updates and renewal of support contracts annually has created extra overhead for the IT Administrator and organisations purchasing team. In addition to this having multiple vendor subscriptions has also lead to the "scape goat" excuse which allows vendors to blame their counterparts when something goes wrong. The firewall vendor blames the antivirus vendor for the virus not being caught and attacking the network, and the antivirus vendor blames the web filtering vendor for not blocking the user from going to the site that the malware, Trojan or virus originated from, and so on.

In more recent years the UTM solution has been developed. The basic UTM solutions that where originally offered to customers provided IT managers a single gateway solution for gateway virus scanning, web filtering, mail filtering and Intrusion Prevention Security (IPS). This is a cost effective method to securing the network without additional administration requirements, multiple support contracts or knowledge of a wide variety of vendor's products.

These UTM solutions are considered to be a wise idea for small operations with a minimum number of users and not considered for anything over a small office user base. The Enterprise market space are still considering the multi-vendor multi-tier solution to fulfil their security requirements.

Firewall UTM solutions have changed over the past few years. The UTM services do still tend to be OEM bolt on services from alternative vendors but further services, usually created and developed by the firewall vendor themselves, and started to surface. For example, certain firewall vendors have started to offer website reputation defence services. These services are in addition to the web filtering policies that may have been created on the firewall. The reputational service queries a database, usually held in the cloud, and checks each website visited to verify the legitimacy and content of the site for any malware. Malicious users or hackers are now, more often than not, targeting benign sites to spread their malware, viruses and Trojans via drive by downloads. The reputational defence allows your firewall to determine whether the site being visited contains malware, or suspicious content, and blocks the user from visiting these sites until such time as the reputation rating diminishes.

Having the UTM service at the gateway also provided a central reporting tool for all activities, security based, that the UTM solution provided. The IT Manager has been able to provide management reports to directors and other board members of security threats, unauthenticated attempts to access the network, and usage reports based on what staff members have been surfing. These reports can also be shared with HR and staff member's line managers to monitor the performance of staff members.

The UTM models of past however have had fundamental flaws. These flaws are that the firewall vendor is still relying on OEM bolt on solutions rather than developing solutions in house themselves. There are obvious and inherent issues with a firewall vendor, or other security vendor, suddenly changing tact and developing an engine of their own to offer a UTM service, however, there are certain vendors who have managed to get round this problem.

Certain vendors have acquired organisations over the past few years which has propelled their solution into the realms of a "true" UTM solution.

Organisations that have acquired companies have managed to integrate the solutions acquired into a single UTM platform, branded under a single badge, and offer a service whereby the firewall element is run by, and developed by, the firewalling branch of the organisation, the web and e-mail filtering solution, again, is run by, and developed by, the web and e-mail filtering solution, and so on.

Again with the UTM's of past, this offers a central security solution which enables the administrator's ability to set policies for traffic inbound and outbound along with reporting on all security related matters that occur.

These new breeds of UTM appliances also offer a central point of management for additional security services that the older security platforms neglected. These area include the endpoints (PC's, servers, laptops, etcetera) along with wireless infrastructure deployment and management.

Deployment of these UTM solutions can also be done in a staged approach. From a financial perspective the IT Manager do not need to worry about ripping and replacing the entire security estate all at once. A staged approach of replacement of solutions as they expire can be undertaken.

Exemplary Scenario

End user's existing infrastructure lists as below:

- Cisco ASA firewall at the gateway
- Trustwave M86 Web Filtering solution
- Barracuda Networks Spam & Virus Firewall
- McAfee Anti-Virus
- NetGear wireless infrastructure
- PGP hard disk encryption with Universal server for central management

In this scenario each of these solutions would typically have had to have been deployed and managed individually. Each solution would have its own maintenance contract, and each of these would potentially be due at a different time in the year. All policies would have also have had to have been set up individually. Due to the security nature of these solutions the vendors have not created these solutions to talk to each other and so therefore there may be potential conflicts within each solutions policy.

As each of the solutions above become due for renewal an alternative should be considered in order to become a full UTM house. An example of the solution that an IT manager could consider would be as follows:

- Sophos SafeGuard for Encryption of the hard drives
- Sophos AP 30 or above for the wireless infrastructure
- Sophos Endpoint protection for antivirus on the servers and desktops
- Sophos Full Guard licensing for Web and E-mail filtering
- Sophos UTM Firewall Appliance for Firewalling and central management

If the example above is deployed from a top down basis then once the end user deploys the UTM firewall this will automatically create the full UTM, centrally managed, infrastructure solution as explained throughout this article.

This solution, on an annual basis, would also save the it department a considerable amount of their budget which then frees this extra amount of yearly spend to be used for other vital areas of the network.

Additionally the firewall hardware solutions on UTM services, which is used for the central management and reporting, can also typically be in either a software or virtual version. Being able to deploy this solution in a virtual environment, or as a software deployment, again saves on the amount of hardware on the network. This means that there is less hardware that could potentially fail, the cost of hardware replacement warranties on kit does not exist and backups, or failovers, can be easily deployed with the minimum amount of work from the IT administrator.

The new breed of UTM solution also lends itself to being able to secure larger Enterprise style organisation's networks. The individual solutions, integrated and re-branded under a single banner, are all in their own right Enterprise solutions and have been deployed in the past in the old school multi-vendor/multi-tier scenario for years. Now these are all under one umbrella it means that the Enterprise market space should readily welcome UTM as a platform for securing their networks too as this new age of UTM becomes more prolific.

Summary

In conclusion, the method of securing the network infrastructure with a multi-vendor/multi-tier approach has now been over taken by a single-vendor/multi-technology scenario offering a more cost effective solution to both the small to medium and enterprise sized business with central management, reporting and control.

"Less hardware, less to go wrong, less cost, more secure."

ALEX MARTIN

Alex Martin is a Network Security Consultant with many years of experience working with a multitude of IT Managers from various industry types throughout the UK. A focused individual with particularly strong experience in high user volume solutions. A no nonsense and yet unbiased opinion allows for an honest approach to customer/vendor relationships.

ForeScout Technology Mobile Security Software

According to latest market statistics, smartphone and tablet devices will outnumber personal computers by 2013, becoming the most used devices for accessing Internet, processing and storing personal data.

RIFE
Research Institute of Forensic and E-Crime

Some of the newest models have the same features and hardware capabilities of a normal laptop, such as: fast CPU, large storage, microphone, high definition video camera and display, network connectivity and so on. For those who still ignore the potential of these devices, it is worth pointing out that they can also be used to access and manage: bank accounts, sensitive data and any other kind of personal information stored or processed within the device. This aspect makes these *Jewels of technology "the perfect target for hackers and malicious attackers". Mobile devices together with applications and Cloud services may represent a lethal cocktail of security threats, exposing users to a number of critical risks that may result in financial and reputational impact. More so, personal mobile devices are being brought into the workplace whether organizations like it or not, or are even prepared for them. The term "IT Consumerization"is top of mind as companies need to reckon with how to allow more secure use of these devices.

Mobile Communication Threats

There are a number of possible threats that a malicious source may attempt to exploit on the users or the vulnerable application and design weaknesses of the device.

Accidental or intentional Data leakage: a stolen or lost mobile device without effective protection, may easily grant access to data. The device may also be thrown away, or transferred to another user without removing sensitive data. And the device may be used at the enterprise to access network resources and company data.

Rooting: Power users may want to customize their mobile device by way of a root kit, which are easy to come by. In the process, the user can potentially eliminate or expose the mobile OS safeguards.

Phishing: Social Engineering techniques or malicious code may allow an attacker to collect and steal user credentials (i.e. passwords, card numbers, SMS or email) and personal identification data.

Network spoofing attacks: A malicious attacker creates a fake Wi-Fi access point to the network and users connect to it. The attacker intercepts the user communication and develops further attacks.

Spyware, Software surveillance, Dialer-ware/Malware and other Viruses: Spyware and Surveillance software are malicious programs that allow an attacker to spy and control remotely the target machine. These types of programs are also used for data theft. A malicious source may attempt to steal money using hidden Dialer-ware that activates SMS services, or calling specific numbers.

There are malware designed to steal credit card numbers, login credentials for online banking and e-commerce.

One of the biggest areas of concern for mobile device security is the workplace.

Personal and corporate provided smartphones and tablets are increasingly accompanying or replacing laptops and PCs as a normal way for employees and contractors to perform their job. This has changed the very dynamic to address protection strategies and mechanisms. This is where ForeScout Technologies mobile security solutions mission starts.

ForeScout Security Platform

I am currently employed as IT Security Engineer and Risk Analyst for a large financial institution and as part of my roles and responsibilities I have to evaluate security software and solutions. Some of the tested Applications are well designed but practically not able to deliver (apart from the amazing description of inexistent features and capabilities, readable on the Marketing slides) the fundamental elements of quality, reliability and manageability, expected within a critical environment, where protection is a primary concern.

During the years I have developed an educated skepticism for the exciting promises and enchanting descriptions delivered during the initial phase of a product proposal and evaluation. Now I tend to approach reviews inspired by a religious zeal, using the proverbial incredulity of Saint Thomas.

I have been invited by HAKIN9 to review ForeScout Security products and surprisingly I must admit that there was much more to the product than the usual enchanting marketing slides.

Let me start by describing what ForeScout technology is, what they propose as Security solution and how Users and Organizations may benefit from ForeScout products.

ForeScout is a leading provider of automated security control solutions for enterprises and government organizations. During the Live Demonstration, a senior *sales engineer* (SE) at ForeScout gave me the opportunity to explore and evaluate some of most important applications and features provided by ForeScout. Specifically we've tested ForeScout CounterACT NAC (*Network Access Control*), ForeScout Mobile Security Module, ForeScout Mobile Integration Mobile (CounterACT plug-ins) and ForeScout MDM (a custom version of MaaS360, the full mobile device management system by Fiberlink).

CounterACT NAC is a product that allows an organization to control how all users, systems and devices, including mobile devices and VMs, access network resources and applications, gaining complete control over network without disrupting corporate and end-user productivity. This application can dynamically remediate violations, such as an unpatched system, out-of-date anti-virus, a misconfigured personal firewall, or de-activated encryption software, operations intervention. Everything is contained within a single appliance that integrates into one's existing environment. CounterACT can also identify and provide network-based control mechanisms for managed and personal mobile devices.

The Test Lab

For this Review we have tried to equip our lab to be as close as possible to a typical production environment. The test area network had about 130 Servers remotely connected and running different Operating Systems versions such as: Microsoft Windows (Ultimate, Professional and Server 2008) and Linux (Ubuntu and Red Hat Enterprise). The network was divided in 8 different VLAN / Subnets, managed by 2 Routers + 3 smart Switches. Network is comprised with Servers running DNS, DHCP, LDAP/AD, email server and few more common services. Moreover we had 2 instances of Apache Web server, 2 Oracle instances + 2 SQL servers, 3 different Firewalls + IDS, 3 Antivirus Servers, 1 VMWare ESX, 1 Microsoft Hyper-V and few Android and Apple devices connected Wirelessly. On top of this I have my personal Laptop with a Linux BackTrack connected, just to investigate a little deeper.

Pre-installation steps

Prior to installing the software and related plugins, there needs a bit of planning. The appliance should be deployed in a network position where all the network devices can be reachable to ensure all connections to the network (local and/or remote) are monitored and controlled by the CounterACT solution

The installation

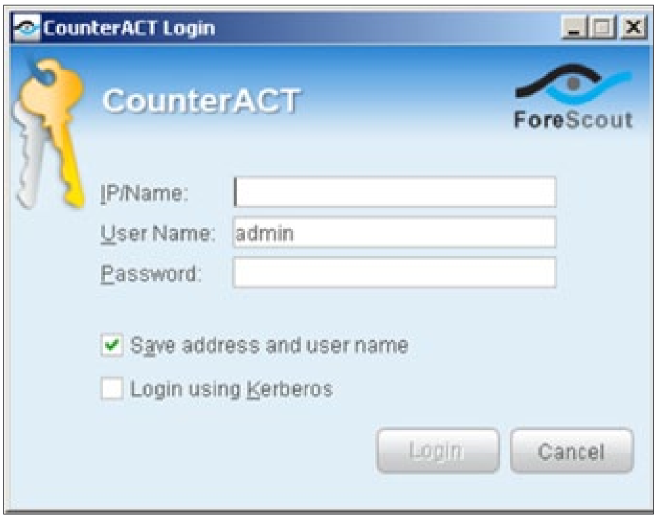
We have performed a full installation of CounterACT Virtual instance (CounterACT Appliance is available as a physical hardware component) on a normal Laptop with a Microsoft Windows 7 Ultimate running VMware ESX, without any specific hardware or software requirements (note that the system did not meet ForeScout's VM specifications). One of the first things I have noticed was the professionalism of ForeScout's SE. This is very meaningful to me, a remarkable quality element. SE's represent the Vendor presence and reputation on customer sites, thus it's extremely important to provide skilled and professional resources.

The second remarkable thing was regarding the installation process. Commonly these NAC applications are complex, with a number of pre and post-installation steps to perform. Well, CounterACT is an integrated Appliance, thus, there is no need to struggle with different components, agents deployment (note that agents are optional), Database installation or other time-consuming configuration settings. Network availability checks, some licensing work and we were ready to install the CounterACT Management Console. The console is built into the appliance and is the central management application used to view, manage and analyze the activity detected by one or more CounterACT Appliances.. It's easy enough to open a browser connect to the appliance IPAddress and follow the screen instructions. (Other installation methods such as: CD, DVD are available). The first impressions I had of the Console GUI was definitely of friendly interface, intuitive and easy to manage. We've verified that all the critical connections that CounterACT uses to perform tasks, may benefit of SSL encryption.

The System Access Security

Access to the systems and protection Models are some of the first concerns for security experts in regard to the security of an application. Especially when sensitive information and critical management settings can be performed using a high level of permissions.

CounterACT login system can be fully integrated within the local or remote MS AD, RADIUS, TACACS, and any user-defined LDAP server. It is also possible to install and manage the user accounts locally using an integrated Database as credential repository. We decided to use our own Active Directory Service, thus we were authenticated and granted access, quickly, securely and successfully.



IP/Name:
User Name: admin
Password:
☑ Save address and user name
☐ Login using Kerberos

Figure 1. *CounterAct Login window*

The software design provides a RBAC (Role Based Access Control) access control mechanism with a policy management server built into the appliance. This provides a good granularity over the permissions management and enables a wide operational control, enforcing the overall security (Figure 1).

Network Access Control

CounterACT NAC automatically started a thorough inspection over the entire Area Network (we report not much impact on Firewalls and IDS) it progressively started to populate the console with all the discovered objects creating a visual inventory. We have detected both active and passive scanning activities using Network monitoring and detection applications. Apparently, as long as the device has an IP address or is connected (Wireless or wired) to a device with an IP address it will be detected and presented within the inventory available on the management console. The only device that CounterACT was not able to detect was a completely passive Ethernet line tap (Figure 2).

The system automatically updates the existing online inventory once a device attempted to connect to the network. So the inventory templates (which can be customized) classifies all discovered devices and related details such as user, location, and configuration as discovered. Policy templates determine if the device should be allowed, limited or blocked from access on the network, or if some configuration element should be fixed based on what is discovered and the access policy. Using the built-in manageable policy and other features, CounterACT was able to identify and distinguish if the access that was requested and performed was from a "good" or a "bad" user/device. Guest management is also a part of the system but was not tested here.*ForeScout Mobile Plug-ins***.** The following step was to install and evaluate. The ForeScout Mobile Security Module extends CounterACT's level of control granularity with regards to Android and iOS security. It is comprised of an XML file added to the CounterACT system and a lightweight mobile app for Android (and iOS) devices. The Android application collects information for each device on which it is installed and reports this to the appliance. This allows determining the compliance of the Android device, restricting network access on the basis of that information, and sending automatic notifications to users to help them remediate policy violations and security problems, such as password, encryption and application requirements. CounterACT can also send requests to the mobile device that is similar to that of MDM systems. We have done similarly for iOS Module on iPad and iPhone. With iOS, CounterACT uses Apple's live push and MDM services which is implemented through a Profile accepted by the user on their iOS device. This allows organizations to automatically find unmanaged corporate (or non-corporate) iOS devices and make them manageable/visible to the network security and policy compliance teams. Here too, a broad number of security features can be managed. There is also plug-in also allows for interoperability with other MDM systems – Fiberlink was tested. *ForeScout MDM (Mobile Device Management) MaaS360 by Fiberlink***.** During the review, we have noticed that this was looking as an external product, then the SE gave us some background information regarding their ForeScout MDM solution. This product is part of a partnership with MDM SaaS developer Fiberlink that gave life to a fully integrated MDM and network access control (NAC) solution. MDM incorporates a customized version of Fiberlink's MaaS360, a cloud-based management system for smartphones and tablets, working with client-side software that installs as a profile on IOS devices and as a mobile agent on Android through a self-guided process. The software seems to be also available for BlackBerry and other platforms. CounterACT has a connector to the MDM which allows the NAC system to gain a much greater degree of visibility and control of all mobile devices controlled by the MDM. ForeScout MDM is cloud-based and offers lifecycle management from enrollment to securing device data and applications, providing the ability to remotely locate and wipe. While ForeScout MDM managed MDM controlled devices, CounterACT can apply network-level controls to unmanaged and MDM connected devices. It detects in real-time unidentified devices attempting to enter the network, and it can automatically implement controls to block, register as guest, push into an HTML for virtual desktop enrollment, or enroll via MDM on-demand with full device inspection and agent deployment. The benefit being threefold: controlling unmanaged devices, enrolling devices into MDM, requesting the MDM to check the security profile of the device on network entry, and to control what network resources an MDM-managed device can access (Figure 3).

The screenshot above shows the Console GUI we have installed on the test machine. We have immediately familiarized with the available menus, trying to run and activate some of the integrated options and Tools.

Testing phase

Using both Policy base and Manual processes, we went through a number of tests, on IPad and Android mobile devices. We've evaluated some of the most critical scenarios as well as the effectiveness and manageability of CounterACT with ForeScout Mobile and ForeScout MDM (Maas 360).. Non-cor-

Figure 2. *Device detection*

porate, external or personal device connection and authentication over internal protected networks is extremely dangerous and should be monitored and restricted. CounterACT NAC + MDM provides this functionality.

Automated enrollment

A device was connected to test network and checked for manageability by CounterACT. The device was prompted to install a profile, demonstrating the streamlined process of managing the device OS.

NAC – hijack and request network credentials

An initial test was performed trying to connect a device to our test network via Wi-Fi, attempting to access the Internet. The device was hijacked and requested to authenticate against the access control system, demonstrating the ability of the software to control network access by requiring non-corporate devices to authenticate.

- The device joined Wireless Network
- Matched "Network Authentication" Policy and an HTTP Authentication Actions committed to the endpoint.
- Received the HTTP Authentication prompt and logs using demo/demo credentials.
- After the successful authentication, network access was provided.

Using the pre-configured policy, the software successfully Hijack the BYOD and non-managed devices and apply the corrective action.

Testing Policy – Camera disable

We've created a rule to disable camera on manageable device. Joining the test network, the device was firstly checked for manageability by CounterACT and subsequently was prompted to install a profile.

The policy rule forced the device to disabled the camera, demonstrating the ability to interact with the mobile device and apply restrictions to applications.

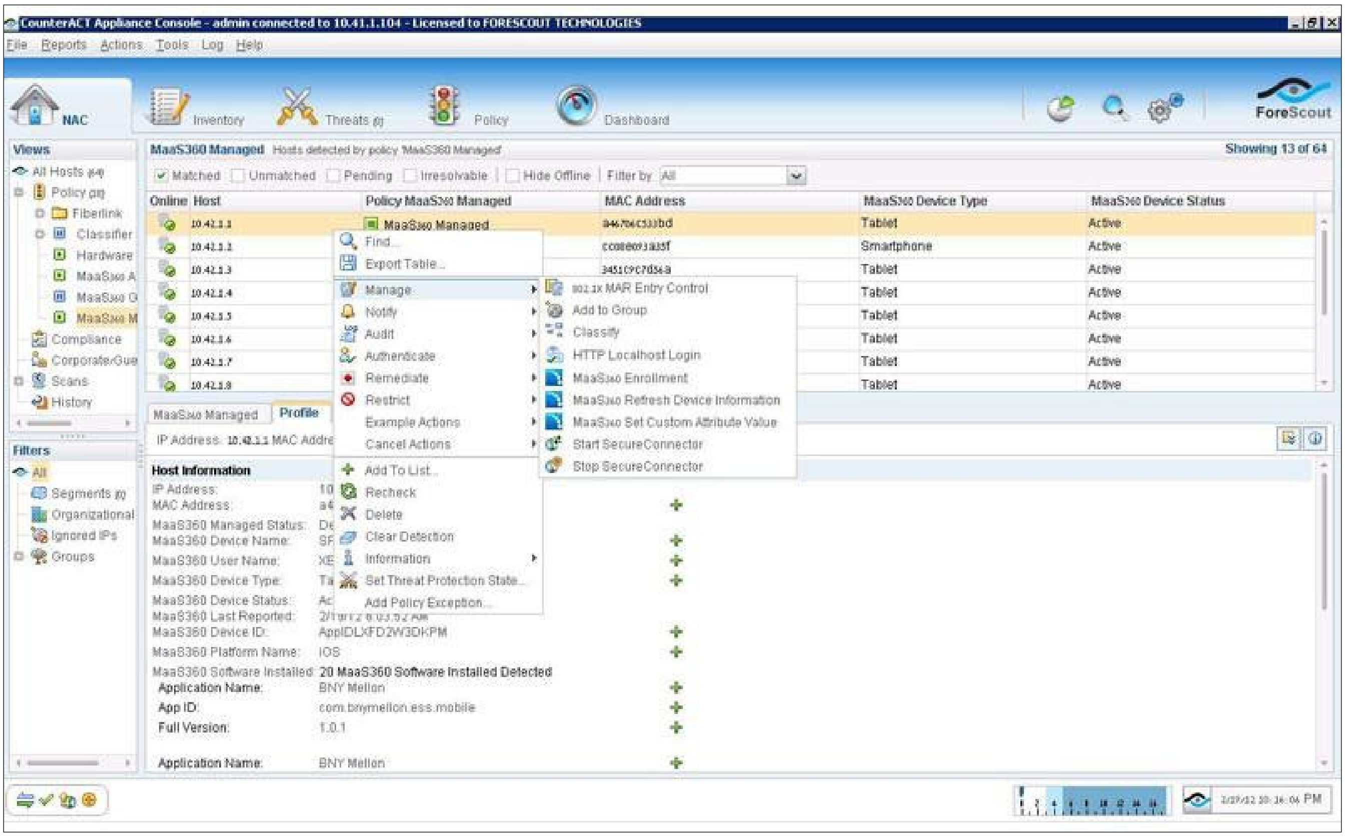
We've successfully tested the same scenario running the process manually.

Adding web clip to the mobile device

On the same device was pushed a web clip linking an icon on the home screen to the ForeScout web site. The device matched an iOS Manageable Non-Compliant sub rule and an action adding a policy to deploy a web clip was applied. As matter of fact, the device received a new icon on the home screen linking to *www.ForeScout.com*. The same process was successfully performed manually.

Device access configuration management – password

A manageable device was required to utilize a screen lock password, to demonstrate the abil-



MaaS360 Managed Hosts detected by policy 'MaaS360 Managed'

☑ Matched □ Unmatched □ Pending □ Irresolvable | □ Hide Offline | Filter by All

Showing 13 of 64

Online	Host	Policy MaaS360 Managed	MAC Address	MaaS360 Device Type	MaaS360 Device Status
✓	10.42.1.1	MaaS360 Managed	a4670dc533bd	Tablet	Active
✓	10.42.1.2		cc08e0931a35f	Smartphone	Active
✓	10.42.1.3		3451c9c7d3e8	Tablet	Active
✓	10.42.1.4			Tablet	Active
✓	10.42.1.5			Tablet	Active
✓	10.42.1.6			Tablet	Active
✓	10.42.1.7			Tablet	Active
✓	10.42.1.8			Tablet	Active

IP Address: 10.42.1.1 MAC Addre

Host Information

IP Address:	10
MAC Address:	a4
MaaS360 Managed Status:	De
MaaS360 Device Name:	SF
MaaS360 User Name:	XE
MaaS360 Device Type:	Ta
MaaS360 Device Status:	Ac
MaaS360 Last Reported:	2/1[illegible] AM
MaaS360 Device ID:	ApplDLXFD2W3DKPM
MaaS360 Platform Name:	iOS
MaaS360 Software Installed:	20 MaaS360 Software Installed Detected
Application Name:	BNY Mellon
App ID:	com.bnymellon.ess.mobile
Full Version:	1.0.1
Application Name:	BNY Mellon

Figure 3. *Managing in CounterAct*

ity to enforce security configuration. The device matched an OS Manageable Non-Compliant sub rule and the action to add a policy to enforce a screen lock was applied. We have verified that the device prompted to choose a password. Based on the same principle but adding some new policy we could also successfully create a strong password policy and application restriction.

Selective Wipe

We tried to remove the profile of the device from CounterACT console. This was blocking the device from any further access and action, demonstrating the effectiveness of the policy and profile configuration. We could evaluate that policy and profiles are customizable by users and groups, providing a large number of configurable permission and access type.

Using Virtual Firewall to quarantine non-compliant devices

We have applied a CounterACT virtual firewall rule on a device with access granted to verify the firewall restriction effectiveness. The device dropped out of network connectivity and Internet access. We have then determined how Virtual Firewall was committing such actions. Apparently, VFirewall uses packet injection and TCP reset mechanism to dynamically control network traffic. Essentially, using a TCP reset mechanisms, which send the RESET to the source after the data is already on the wire and sending the RESET to the destination after the first SYN, tearing down the connection before the handshake completes. We've tested trying to reset a TCP connection of a joined device. As result the device lost the connectivity. Other enforcement (see ACL) is available but this method enables enforcement without any infrastructure changes that for some organizations would be compelling.

Appendix 1

Materials/Documents provided by ForeScout

- Overview of NAC (by EMA analyst)
- Overview of CounterACTplatform
- Overview of market (by Frost and Sullivan)
- ForeScout CounterACT datasheet
- ForeScout Mobile datasheet (this is the mobile security plug-in)
- 451Research report on ForeScout Mobile

PDF

- FS-Abridged-NAC-report.pdf
- ForeScoutMobile_the451.com_-2.pdf
- ForeScout-Mobile-Datasheet.pdf
- Tolly212105ForeScoutComparativeNAC.pdf
- FS_Overview-Dec2011-FINAL.pdf
- EMA_AchievingNACResults.pdf
- FSCounterACT_Eval_Guide_2011.pdf
- ComputerTechnologyReview-CounterACT-Aug2011-web.pdf

Video

https://www.youtube.com/watch?v=QxMsU7lt5sc

ACL enforcement

We have enabled and tested ACL Enforcement on: Firewall, Router and Switches within the test network. We have configured a specific ACL rule to block access to a specific port. We have then changed the ACL settings to roll back and to perform access using the same port. All the tested configurations were successfully verified.

Conclusions

We have spent many hours in our test Lab going through the extensive range of checks and verifications on ForeScout products, we have also tried to find potential bug or gaps on CounterACT to verify how easy it could be for an expert user to exploit a vulnerability on CounterACT NAC and ForeScout MDM, but we failed.

In our opinion the integration of CounterACT NAC, its Mobile add-on modules and FS MDM, had demonstrated to be a valid and effective end-to-end Security solution, addressing network access and mobile security concerns and delivering total control over the managed network and devices using:

- Detection
- Monitoring
- Protection
- Administration
- Remediation

We believe that ForeScout products are able to satisfy the network access and endpoint security exigencies of corporate and governments but at same time the increasing request of mobile security, triggered by the wide use of smartphones and tablets.

ABOUT THE EVALUATOR

SEMBIANTE MASSIMILIANO
IT Sec&Risk Eng. at UBS Bank
M.Sc. Computer Security
Can be reached at: msembiante@rifec.com

Interview with Alex Kirk

Alex, a member of the SourceFire Vulnerability Research Team and leader of SourceFire's AEGIS Project, especially for Hakin9; He discusses malware, threats network security techniques and settles the score once and for all – Star Wars or Star Trek?

Hakin9: First of all, the first question. Would you like to tell our readers about your professional background and technical education stuff?

Alex: Sure. I have a Bachelor of Arts degree in Computer Information Systems from Strayer University, but honestly that's not all that relevant to what I do at the end of the day. What I've really found is that most of the really good people in the computer industry and in particular in security industry are self-taught they have learnt things as they've gone along through the years. I think I fit that model better. I had a Sega DreamCast – the old video game system that I ran NetBSD and a Mixmaster anonymous remailer on for a while, just because it was fun to learn how to do it and I could support free speech at the same time. For me, my education has primarily been going out and figuring out how to get things done. As far as, you know, professional background, I was a webmaster and technical writer contracting to the United States Department of Agriculture for a couple of years, and was laid off actually around September 11th. So I was an unemployed webmaster in 2001. Then, after a brief stint in a commercial real state firm doing research because that's what paid the bills, I ended up getting outsourced there as well. I came on to SourceFire about 8 years ago, and have been with Vulnerability Research Team the entire time. It's been an excellent place to work. I've really learned a lot in those 8 years and I still have a lot fun doing it.

Hakin9: What about your role at SourceFire and would you like to share with us your exciting projects there?

Alex: (Laughs) So, so the Vulnerability Research Team is the group that produces the Snort signatures, so we are the guys that have to understand a given vulnerability or a piece of malware or whatever so then we can actually do proper detection for it. My role..I originally started as just a Junior Analyst here, set up systems for so other people could break into them, and learned a great deal about computer security in the process. I've been writing Snort signatures the entire 8 years now. Currently I am the lead of the Source Fire AEGIS Project, which stands for Awareness, Education, Guidance, and Intelligence Sharing.

Hakin9: Could you expand on that topic?

Alex: So what that program is, we came to the conclusion a couple of years ago that we had a lot of good information about vulnerabilities in the wild, be it from the feeds that we get or paying attention to Milw0rm or PacketStorm or places like that. And while we understood the threat landscape reasonably well, we didn't have any feedback at all from customers or even just Snort end users about "Was that detection that we are producing as useful as it could be for people?". Because, you know, in reality-last year they were over 5 000 CVEs, just in 2011 alone. No ??? IDS company produces protection for all of that because you can't do that much detection at wire speed, realistically. And so you've always got to kind of make choices about what kinds of things you are covering. And sometimes it's obvious, the remote desktop vulnerability that came up this Tuesday (CVE-2012-0022) is very much more looking worm-able this point, we've got detection for that clearly because it's relevant. But you know, sometimes it might be SQL injection in some sort of a web system that you don't know that anybody necessarily uses. I got tapped through this AEGIS programme as the guy to go out and solicit that feedback from customers, to have conversations with people about "Are the [Snort] rules working for you, are there things that we can be doing better, what is your view of the threat landscape?", so we actually make sure that what we are doing is useful out in the field. That entails a fair amount of travel around the world to talk to different people, speaking at conferences, that sort of thing. I actually did 16 countries last year – I did a variety of conferences, including the CARO Workshop in Prague, which is the Computer Antivirus Research Organization; You Sh0t the Sheriff and Hacker 2 Hacker in Sao Paulo; Ekoparty in Buenos Aires; Hack in the Box Malaysia in Kuala Lumpur, as well as Ruxcon in Melbourne, Australia.

Hakin9: Ok. Knowledge of latest threats and attacks is critical in Vulnerability research, how do you keep up with such a fast-moving landscape?

Alex: That's part of why we have this AEGIS program – its purpose is to actually talk to our customers and ask what it is that they are seeing out in the field. We get good data from Microsoft on many things, and we work with a number of other groups directly on vulnerabilities they have seen. We also pay a lot of attention to what we see in the community; there are different websites that we follow. Funny thing is Twitter is actually a really excellent medium for staying on top of security. If you follow the right people, they've got really good links all the time and you can learn about things before it hits any kind of maistream media.

Hakin9: Well, nice... Nice to know. Intrusion Analysis and Detection is one of the old techniques in network security, what are some of the advances in this field?

Alex: I actually have to dispute the notion that intrusion analysis and detection is old school. Yes, it's been around for a while, but the reality is you're always going to need to understand vulnerabilities in order to detect exploits against them. That is, you know, that's what the difference is that we find between SourceFire and other IDS providers out there, that we really make a point to write a signature for the underlying vulnerability and not just a particular exploit against it, so that is doesn't matter what piece of malware or what attack is being used. If you get – if you see, "What are the key underlying criteria necessary to hit this vulnerability, then you're going to be detecting all of them, regardless of how they're implemented. One of the cool things that Sourcefire is doing that I've been involved in is some work in the malware industry. In January 2011, Sourcefire acquired a company called Immunet that made a desktop antivirus product, and when I first saw that, I thought, "Why in the world did we did just do that?". I was confused because we sell to enterpirises, government, large organisations, and not end users. Essentially, what we were doing wasn't so much acquiring an antivirus company, as buying a really awesome cloud infrastructure that happens to have an antivirus product attached to it. So that is now turning to an advanced anti-malware platform, and esentially what this is, it's an agent that sits on the desktop, takes about 20 MB of memory – so a much smaller footprint than traditional antivirus – and any time the user attempts to execute or create a new file on the machine, it sends a 100-byte UDP packet up to our cloud. Ninety-five percent of the time the cloud says, "Oh, I know this, it's winsock32.dll, let it run," or "Oh, this is a known piece of malware, block it." In cases where it's not familiar with a given new file, you've got a heuristic process that the cloud goes through for new samples, that's been developed by our researchers for the last couple of years, that will make a decision on a spot based upon things like "Does this have kernel hooks? What kind of network ports does this thing open? What sort of files or registry keys does it create, or delete, or modify?". There is a whole sequence of things it will look at and it can, really fairly accurately, make that decision as whether or not something is malware or not. The cool thing about that is not only are you catching new stuff on the spot, but if a new file shows up in Singapore, let's say, at noon – and then that same file shows up here in Warsaw at 12:01, the cloud already knows about it, you don't have typical desktop antivirus lag, where you can go up to a week in between a sample coming in and being analyzed and detection actually coming out to users. So, you know, between that and data that we are staring to collect on the rate of the traditional IDS signatures firing in customers' live environments, we are actually launching a programme to put SourceFire-owned sensors on customer's networks that go back to the VRT labs' control management centre. We are getting a lot better insight into what is actually active in the threat landscape, what are the things we need to focus on, what sources of information we need to start pay attention to as we look forward.

Hakin9: You have presented on Mobile Malware. What are some of the threats of today and what are your mitigation techniques?

Alex: So mobile malware is interesting because it's new. So to put it in perspective, SourceFire also owns ClamAV, the open source antivirus engine, so we have a giant malware database with millions of samples. We of course trade samples, just like everyone else in the industry does. So we get about 150 000 unique pieces of malware a day into this database. When you look at that, we only have about 2,000 total samples for mobile operating systems, so the percentage of malware out there is actually running on mobile platforms is just absolutely tiny compared to the traditional Windows desktop side. Today it represents a very small portion of the threat landscape. (*Michał*)What we are doing to deal with it is "on the spot" analysis of things whenever a new threat pops up so we can produce IDS signatures if necessary. The FireAmp product – they're going to have an Android client (*Alex*) Honestly, what I would say for most users – you need to just stick to the official market for iPhone, Android, or whatever, because the threats we are seeing out there are generally in alternative marketplaces. If you go to some website and download a random APK file, chances are way, way higher that you're gonna get hit with malware than if you are going to the official Google store.

Hakin9: You are experienced in running malware sandbox, can you tell us about that? Your key observations, challenges that you might have come across?

Alex: We actually have two different malware sandboxes that the VRT runs. The first of them is the one that I actually built myself. It was essentially just ESX servers with a whole bunch of WindowsXP SP2 unpatched boxes. The idea was if there's anywhere modern malware's gonna run – it is definitely XPs SP2. So basically, I just scripted the process of taking a sample out of the ClamAV database, dropping it into the ESX box, forking off tcpdump in the background with a BPF specific to the virtual machine that was going to run the malware, and then executing it on that VM. I let each sample set for 200 seconds, and then revert back to the clean snapshot. That essentially captured network traffic on these things. That has been a very useful tool for us, because we can look at trends in terms of URL patterns or different host names, things like that. We also have very good data about ephemeral, low-TTL vs. long-term threats. It is a little challenging from an infrastructure perspective just keeping these things fed and cared for all the time. Making sure it does not crash or anything like that. It was not really that difficult to put together. With the inauguration of the FireAmp product we've got the sandbox that uses the Joe sandbox product, which in addition to giving you network traffic, you'll get all the registry keys and files that were edited, modified or created on the system. You'd get screenshots and all the information you'd need for a standard sort of antivirus product, plus all that network traffic. It is giving us a lot more insight into what malware actually does when it is dropped onto a given machine.

Hakin9: Can you explain the technicalities behind giving malware a name? You had some hints about that on your blog.

Alex: Actually, it is not one of my primary responsibilities. As far as I can tell, there's no standard at all within the industry. It is very frustrating when a client says: "Do you have coverage for this particular piece of malware?". I don't know, because I do not know what it is. If we are naming something, and have seen that other researchers have put a name to it, we try to stick to that name. It is sort of centralized and convenient. Actually, within the industry, people stick to MD5 hashes, or now SHA256 hashes, to identify things.

Hakin9: There is a common belief that most malware comes from BRIC (Brasil, Russia, India, China) countries. Any thoughts on that?

Alex: My presentation that I gave in Australia – the Malware Mythbusting presentation – took that on as one of the myths that I was examining.

Hakin9: So, you are refuting the myth?

Alex: Very much so! It turns out that the majority of command and control servers on the Internet, at least according to my sandbox, are in the U.S. If you combine Brasil, Russia, India and China – even those four together don't make up as much as of what is in the United States. I was very surprised to find that, actually, 14 of the top 20 countries by geolocation that are hosting these kinds of servers are very much First World places, where Interpol is present and there is strong law enforcement and all that. I think it is just a matter of, those countries also happen to have really good networking infrastructure to set these things up.

Hakin9: Hence the question about the operation "Shady Rat". It was quite popular about a year ago. Where does it stand now? Do you have any experience in dealing with it or is it top secret?

Alex: I wouldn't say it is top secret. The reality of it is it's not that relevant any more because it's been unmasked. It was a successful operation because it was so sneaky and people were able to exfiltrate data without being observed, but the instant you observe something like that, then it loses its value because people can go and pay attention and get the stuff cleaned off their network. What I found kind of interesting – you remember the Night Dragon malware? McAfee put their report on it out in February 2011. When that came out, I got into the office and was told, "Kirk, go find the copy of this in your sandbox," which I did. I pulled it out, we verified McAfee's claims, and we had a Snort signature out as of that afternoon. But the interesting part about it was that it was straight up binary data on port 80 – no HTTP headers at all. I said: "You know, that's actually not a bad idea if you're going to write a sneaky piece of malware, because every firewall on the planet will let you outbound on port 80 with no questions asked, and if there's anywhere you're going to hide from netflow analysis, it's port 80, because that's where all the traffic is. I wonder how many other pieces of malware are doing this?". I ran that analysis over about a million and a half samples that I had put through the sandbox recently, and it turns out that about 1% of them were actually exhibiting that very behaviour. And funny thing, one of the top botnets that I saw doing that is, actually, run right out of good old Poland here. I've been observing ilo.brenz.pl, it's been up for 2 years now; dropping evil binaries on people, running DDoS networks, just being all sorts of terrible. I'm actually working with some of the guys here in Poland, trying to get it taken down.

Hakin9: Now something less IT-oriented. When you are not analyzing traffic or debunking malware, what is your hobby?

Alex: I enjoy bicycling. My neighborhood has a number of good bicycle trails, one of which actually goes all the way from suburban Washington, DC to Pittsburgh, Pennsylvania. I do that to stay in shape. I also do a lot of gardening. People think it's funny, but, I planted a fig tree, and recently I had a hot tub put in, and the two were close enough that this summer I will literally be able to sit in my hot tub and reach out and pick the ripe figs off of the tree.

Hakin9: Going back in time – what was your first computer?

Alex: I had a TRS-80 model 3 that my parents purchased back in 1984. They actually run a business typing up papers for college students at the time, and so it was a business investment for them. It meant that I could type by the time I was 4 years old. I remember playing Frogger back on the old 8-bit, black and white monitor.

Hakin9: Now teleporting into the future since you are a time zone man – how would you like to describe your legacy?

Alex: It is not something I really thought about. If I am remembered, I hope it's as someone who was able to contribute positively to keeping the Internet clean. No one is going to be able to eliminate all the malware and malicious activity out there. I don't think anyone will ever solve that problem, but if I can be remembered as someone who made positive contributions to that type of research, and helped to keep people safer online, I'd be very happy with that as a legacy.

Hakin9: Any pointers for those who would like to start in the security field?

Alex: Just go out and start playing with things. Get active on mailing lists, any city that you are in is gonna have some sort of a local Linux users group, you might have local hackathons, things like that. Just start doing. You'll be surprised at the number of people who are interested in helping you learn all along the way. I make it a point, actually, when people ask me questions: "How do I do this, how do I do that?", I take the time and give them that kind of information, because I see it as a good karma. I am where I am today because people helped me along the way. I think it is only fair to help others along their path as they get into the industry.

Hakin9: The final question: Star Wars or Star Trek?

Alex: I'm going to have to go with Star Trek, just because I love the idea of exploration. I actually was the webmaster for a group called The Mars Society for a while – we're an international grass-roots organization of scientists and artists, any sort of people who are interested in sending humans to Mars. I have actually lobbied the U.S. Congress in favour of an expanded NASA budget. I even saw a Polish team win prizes at our University Rover Challenge that we hold at one of our simulated Mars bases in the southern Utah desert. I am definitely a huge space nerd.

by Piotr Linke – in the name of Hakin9

Fusic

Fusion of Society, IT and Culture

Fusic Co.,Ltd.

Founded in 2003 in Fukuoka, Japan. Fusic provides several IT related services all around Japan. Among the services we provide are: web development, contract-based software development (such CMS and CRM), etc. We also developed our own web-based presentation service "Zenpre", and e-Commerce platform "Ureru-net-kokoku-tsukuru", and serve consumer through ASP. Currently, we also play a leading role in the mobile applications development in platforms such iPhone and Android.

浜崎陽一郎

Yoichiro Hamasaki
Vice-President
Co-Founder

納富貞嘉

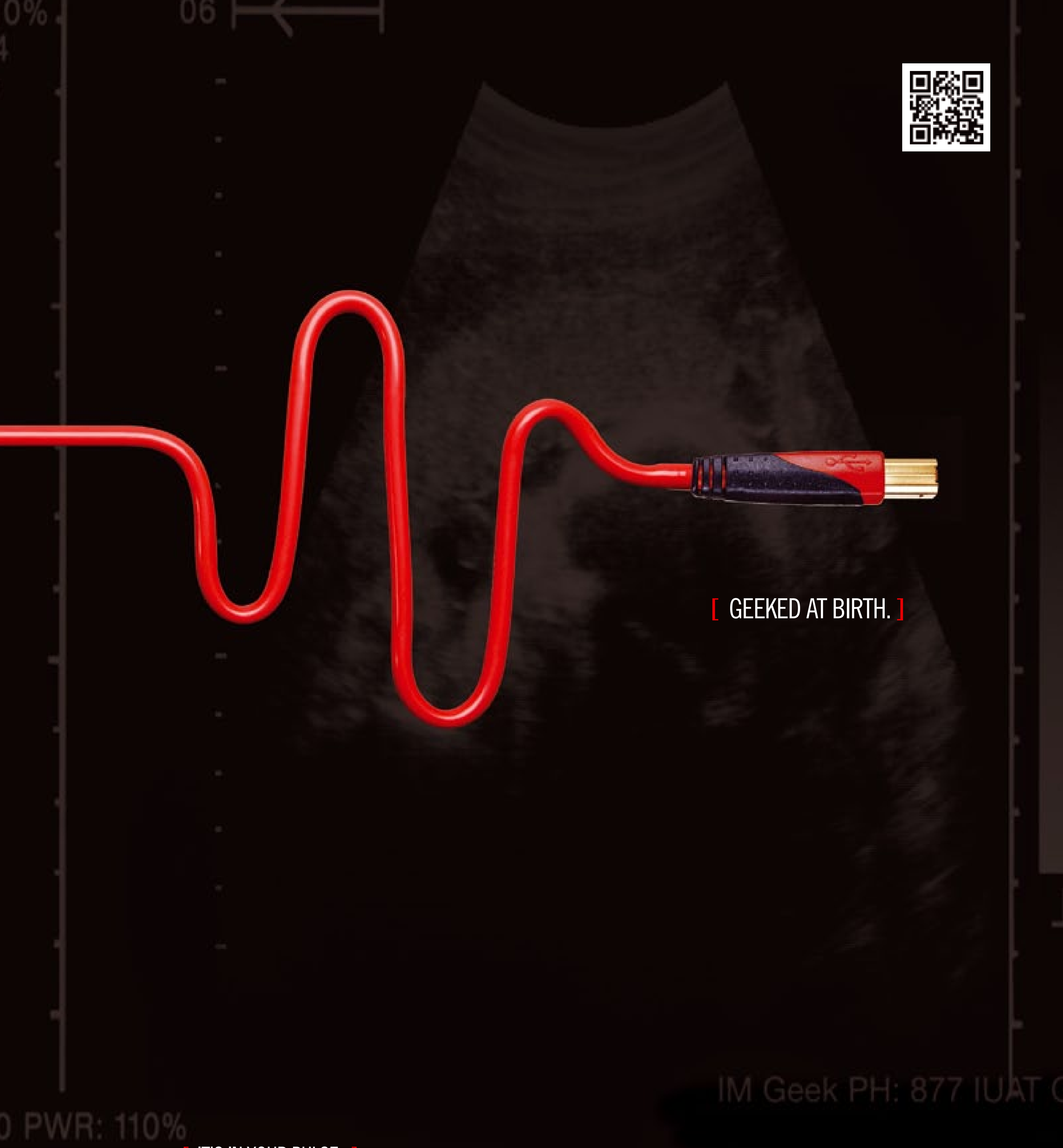
Sadayoshi Noutomi
President
Founder

Fusic Co.,Ltd http://fusic.co.jp/ info@fusic.co.jp

Fukuoka Head Office
Shin-nihon build.9F, 2-4-22 Daimyo Chuo-ku, Fukuoka-shi,
810-0041, JAPAN
+81-92-737-2616 +81-92-737-2617

Fukuoka Laboratory
East Fukuoka General Office 4F, 1-17-1 Hakata Station East,Hakata-ku, Fukuoka-shi,
812-0013, JAPAN

Tokyo Branch
Okura build. 3F, 1-4-10, Shibadaimon, Minato-ku, Tokyo, 105-0012, JAPAN
+81-3-6450-1633 +81-3-6450-1634


0%
06
[GEEKED AT BIRTH.]
IM Geek PH: 877 IUAT G
0 PWR: 110%