100 Tips

for Implementing Network Security

Insight from chief information security officers and those that support them

Stonesoft Press

Helsinki

Contents

Forward

The physical and digital worlds are merging to the point that no one is actually safe without securing their cyber persona. Security online is not an end goal, but an obligation that governments, societies, companies, and individuals must willingly accept from the start. If not, the resulting loss of trust,reputation, property, and wealth could be severe.

Even those not responsible for securing computer networks know that attacks and breaches are rising. The exposure of personal information, including credit card numbers and passwords, is no longer front-page news. The danger we must all acknowledge is that these now common actions can easily escalate to frightening levels. State-sponsored cyber warfare is openly acknowledged with pride by countries that do not have significant physical capabilities to declare war. Even worse, organized crime can attack from locations around the globe, often where local governments are uninterested or where they stand to profit.

Like children that grow up and leave home, the data we once carefully watched over in data centers and mainframes has taken on a new life. It's available everywhere, not only in our phones, tablets, televisions and laptops, but also in our glasses, shoes, cars, bikes, refrigerators, and lawnmowers. A New York woman now has a pacemaker with an IP address, making it easier to enable checkups with her doctor. Data and its associated applications are so ubiquitous that we refer to much of it as existing in "the cloud."

A second wave of innovation that builds upon the commercialization of the Internet is upon us. It is driven by mobility, cloud computing, virtualization, and the new belief by everyone that information should be available wherever and whenever it is needed. More people have smart phones than other types of phones. Almost anywhere you go in a public place you will see half of the heads facing down while they access data.

That brings us back to security. To move so quickly into a new world of data everywhere has left security as an afterthought. Sure, it exists in some form of password and user name combination, but that only keeps out the honest people. Most corporate security professionals will tell you they still battle a lack of basic security education within their employee base. Sticky notes with passwords are still pasted across the desktops of many organizations. Even worse, the rapid application development process and demand for new apps leaves many software development teams struggling to fix errors, leaving security as an afterthought.

The network infrastructure is also changing rapidly. The perimeter is disappearing. It is difficult to put up fences around a cloud. Business managers push data back and forth to cloud-based applications without bothering to include the information technology department. The masters of I.T. are now ignored as more and more solutions are offered without the need for integration with existing legacy systems. Once again, security is an afterthought that comes into play only when the outsourced provider is breached, a disgruntled employee leaves with confidential data, or some other brand-damaging incident hits the news. Security procedures that are now rote in most I.T. organizations are ignored by those not skilled in data security.

What we must protect is now more complex and challenging than anyone predicted. All C-level executives have to be involved in thinking about security first. They must be willing to invest more in operational management, vendor management, and risk management solutions. By putting security first,

the people, processes, and technologies required to implement organizational and technical change will be able to survive these new threats in the cyber domain.

Please read the preface on Offensive Cyber Strategies. Security means protecting ourselves from attacks, and the resemblance of cyber security to military security should not be ignored. We can apply a century of military strategy development to our own information technology strategies, building upon a foundation of defense, resilience, and offense. Dr. Jarno Limnéll illustrates how crucial it is that every individual understands the consequences of ignoring cyber security.

Ultimately, this book should be helpful to double check your plans for implementing security measures across a number of new and emerging technologies. Each chapter reveals insights from practitioners in the field, highlighting hands-on advice that comes only from experience.

Finally, a sincere thank you goes to Stonesoft Corporation for compiling these tips and publishing them for us all. This effort is truly in line with the company's mission "to protect and save lives and businesses in cyber space."

Craig Shumard

CISO, emeritus

CIGNA

ISE Luminary Leadership Award Recipient 2010

Preface

Offensive Cyber Strategies – How to build and expose cyber warfare capabilities to ensure deterrence

Cyber attacks are expected to reach unprecedented capability and distribution in the coming years. As cyber weapons become more complex, and deliberate attacks more frequent, how can security teams take action now to prevent future victimization? Today, cyber capabilities are essential for nation-states and armed forces that want to be treated as credible players.

As the fifth dimension of warfare, cyberspace is an important political arena, and the digital world a domain where strategic advantage can be lost or won.

Contrary to what we'd like to think, succeeding in the cyber domain is not merely a question of defense – at least not for the nation-states. Naturally, defense capabilities have to be as preventative as possible to reduce the effectiveness of an adversary´s cyber attack.

However, despite the best defensive efforts, intrusions will occur. In the cyber domain, you must be resilient enough to withstand attacks and mitigate harm, more so than in other arenas.

Creating cyber defense capabilities and resilience are fairly easy for the public to accept, but are not enough. Deterrence policies that convince others not to launch a cyber attack against you are essential, but are only effective when teams demonstrate offensive cyber capabilities.

Cyber offensive capabilities are a must for nation-states to succeed in the current and future reality of both international and security policies. Defense, resilience, and offense are the foundation of a country's overall ability to protect itself.

From nuclear to cyber deterrence

Deterrence – the art of threatening an enemy with intolerable punishment or unacceptable failure to prevent a specific action – emerged in the 1950s, in response to the new strategic challenges posed by nuclear weapons. During the Cold War, nuclear deterrence kept the United States and Soviet Union in check.

While cyber deterrence should play a similar role in the digitalized world, the anonymity, global reach and interconnectedness of attacks greatly reduce its efficiency. Likewise, nations face suspicion and rumors surrounding their capabilities.

In the kinetic world, it is much simpler to evaluate an opponent's capabilities. We can estimate how many tanks, interceptors, or submarines a given country possesses. Countries also openly expose their arsenal (in military parades for example) and operational skills by organizing large military exercises. In deterrence logic, even more important than having the actual capability is the perception of having that capability.

Awareness prevents conflicts

Deterrence depends on effective communication between a state and the entity it wishes to deter. Much like the physical arena, the strongest states in the cyber domain are those that can respond when

attacked.

More countries openly expose their offensive policies and capabilities to improve their cyber domain credibility – essentially establishing rules for engagement. For example, for the first time since World War II, Germany has publicly disclosed it is developing offensive cyber weapons. Also, the latest Cyber Strategy of the United States emphasizes an offensive cyber policy, and it has been said publicly that the U.S. Defense Advanced Research Projects Agency (DARPA) is researching expanded offensive cyber capabilities. Many countries have also announced that cyber attack responses are not exclusively limited to the cyber domain.

The world's nation-states need to more openly discuss their offensive cyber capabilities and readiness levels – just as they would missile arsenals or submarine fleets. We hear of great military exercises from the kinetic world, but seldom in cyber events. Today, countries are mindful of each other's kinetic capacities – one reason why there are relatively few wars. Awareness prevents conflicts, at least between nation-states, and raises the threshold to conduct an attack. Many countries base defense policies on the assumption that a capable military and willingness to reveal strengths to adversaries decreases risk for attack.

The challenge of attribution

Attribution differentiates cyber warfare logic from that in other domains. Unlike kinetic attacks, cyber attacks leave no physical evidence and can be masked or routed through another country's networks, making attribution a challenge. Even if you are confident an attack came from a computer in a certain country, you cannot be sure the government is behind it. It is hard to deter if you cannot punish, and you cannot punish without knowing who is behind an attack. Moreover, responding against the wrong target not only weakens the logic of deterrence, but creates a new enemy. Terrorists receive openings to engage in warfare formerly undertaken only by nation-states, but are likely only taken where minimal offensive capabilities exist.

While difficult, attribution is not impossible. It requires both technological solutions and diplomacy – namely, deep international cooperation. Countries should plan to establish (if they haven't already) communication channels should something extraordinary occur in the cyber channel. As more countries openly discuss their cyber capabilities and offensive strategies, it will become much easier to approach and navigate political and geographic rules and norms in the cyber domain.

At the same time, some nations are taking responsibility for cyber-attacks to achieve a political advantage and send strong messages of deterrence. For instance, the U.S. government has unofficially admitted orchestrating the Stuxnet attack to show it could use advanced cyber weapons against an adversary – just in time for a presidential election.

Offensive weaponry is needed for credibility and deterrence

The cyber arms race is accelerating, even if we would like to turn a blind eye to it.

Building cyber capabilities relies on quality, not simply quantity. Currently, the most heated race is for the recruitment of talented individuals, and many countries are actively recruiting promising hackers. In all likelihood, so are terrorist organizations.

In most countries, it is not popular or even desirable to publicly discuss offensive cyber weaponry. However, it is now vital that nations explain offensive cyber logic to the general public. Naturally, cultural and national sensitivities dictate how this is done, but in any case, leaders can summarize their offensive strategies in four points:

Defense through Offense

To be considered credible in both the military battlefield and in world politics, you must have offensive capabilities, just as you must have defensive capabilities and resilience. You simply cannot have a credible cyber defense without offensive abilities.

Take Preventive Action

Offensive capabilities are a must to ensure deterrence. The ability to act offensively includes a strong preventative message to others, provided they understand it and believe it.

Strengthen Your Defense

Offensive thinking and building weaponry are vital for creating a stronger, more credible defense. Security teams must understand how an attacker acts, and locate all possible defense vulnerabilities. You must also test your current defense and train your forces. Without the ability to attack, no country can build an effective cyber defense.

Stay Aggressive

When the lights go off, how will you defend with kinetic weaponry against your non-kinetic adversary? In today's warfare, being defensive will hinder achieving your objectives. In some cases, offensive attack is still the best defense. Passive defense alone will not work.

Disclosing offensive weaponry becomes more visible and includes great risks

The secret development of offensive cyber capabilities among nations today is a worrisome trend. Offensive cyber weapons are sophisticated enough to paralyze critical societal infrastructures, endangering human lives.

With such threats looming, deterrence becomes more crucial. Merely talking about offensive cyber weapons will not create the same sense of fear as revealing your arsenal. To show deterrence, nation-states must demonstrate their capabilities without sacrificing the advantage of surprise.

While cyber warfare currently operates under guerrilla warfare norms, change is imminent. As four-star general James Cartwright said, "We've got to step up the game; we've got to talk about our offensive capabilities and train to them, to make them credible so that people know there's a penalty to this."

In the coming years, more nation-states will organize exercises and simulations to expose their offensive cyber capabilities and enhance their deterrent effect. However, in all likelihood this will not be enough.

Nation-states must conduct cyber attacks in real situations and against real targets, such as terrorist or activist groups, industrial plants, or possibly even against other states, and claim responsibility in order to increase their cyber deterrence. In May 2012, U.S. Secretary of State Hillary Clinton announced that U.S. cyber specialists attacked several al-Qaeda recruitment websites. This serves as a strong, deterrent political message of intent to use cyber weapons, and a glimpse into the future of cyber warfare.

Escalation is always a risk when cyber players deploy offense. As history shows, one event can lead to another, and spark greater conflicts. Releasing cyber weapons can also deliver unexpected side effects,

the worst being total darkness of the unpredictable and interlinked digitalized world. Cyber deterrence within the area of operations may be very difficult to limit.

While secrets cannot be used as deterrents, revealing too much cyber weapons information can allow your adversaries to close the vulnerabilities these weapons exploit, and solidify their defenses. Excessive openness can further accelerate the cyber arms race in ways that might be self-defeating. However, deterrence is much more viable if adversaries understand the digital infrastructure is resilient, that credible threat detection and prevention systems are in place, and counterattack mechanisms are ready.

Civilians on the front lines of the cyber battle

Governments and armies alone cannot undertake cyber deterrence. Civilians are on the front lines of the cyber battle every day. Without the proper firewall and anti-virus software in place, attackers can easily overtake and remotely operate thousands of home computers daily. These botnet legions can turn a nation into its own cyber adversary.

Every individual plays a role in building more efficient cyber capabilities, resilience and deterrence. As a result, there is greater need than ever to raise general cyber security awareness, because there is greater potential than ever for advancing a nation’s economy and politics.

Countries will continue building and more openly using offensive cyber capabilities. However, if the general public does not understand how significantly offense impacts defense, it becomes more difficult to openly use these weapons for stronger cyber deterrence. Once the public understands the logic and seriousness of creating offensive cyber weapons, and their potentially devastating consequences, the threshold to use these weapons should rise. Along with that understanding will come what is most urgently needed – deterrence.

Jarno Limnéll

Director, Cyber Security

Stonesoft Corporation

Chapter 1

Ten Tips for Implementing Security Management Securely

Security management is both the armor and preventative medicine for your network that keeps it free from malicious invasions. A major key to effective security management is incorporating a unified front that provides for all your security in one centralized location without the need to scramble to employ various management tools for each security product. Effective management should also provide the ability to share reporting, auditing, logging, and other essential tools to ensure your network remains vibrant, healthy, and infection-free. These ten tips for implementing security management securely can go a long way toward sustaining the life, health, and longevity of your network:

1. Architecture and domains

Architecture refers to the manner in which your security platform is built, with the most effective security management centers containing at least two servers: the management server and the log server. Both can be contained on the same server, or you may opt for two separate servers. A third essential component is one or more management clients, depending on your needs. As with any successful architecture, your management center should be flexible and scalable, with the ability to add components as your business and your needs grow. The same flexibility should apply to your domains, which are components that allow your security management provider to manage customer environments from a central location. You can opt for isolated sub-domains to further keep each customer’s environment intact and easilymanaged as well as to restrict customer admin control.

2. Authentication server

Authentication is a vital tool for security in general, and an authentication server is just as vital for security management. Although technically optional, an authentication server allows you to fortify your network to the optimum degree. An effective authentication server will offer several methods of authentication to best

suit your needs, whether you prefer a username and password pair or a stronger method based on a one-time password sent via text or mobile ID. Ease of use is another major plus with an authentication server, as is transparent integration with existing user databases.

3. Third-party management

Due to the high mobility of today's workforce, any number of third-party devices may need to join your network at any given time. Effective security management is able to manage these device events, collecting log and monitoring information that is then assembled in one central location. This gives you a full overview of what devices are accessing your application servers and exactly how they are obtaining that access. One more plus is a real-time rundown on third-party device usage, which includes stats on disk space, CPU, memory usage and interface.

4. System monitoring and network monitoring

Monitoring your system and your network can make you a harried mess, or you can opt for highly effective security management that offers monitoring options in one unified location. Not only will admins be able to check out the network at a glance, but they will also get the rundown on third-party devices. Effective system monitoring allows firewalls, IPSs, VPNs, SSL VPNs, and servers to be checked, double checked, and viewed when and as frequently as deemed necessary.

The same holds true for network monitoring, which should provide an immediate and real-time summary of network data. Find a network monitoring component that provides traffic statistics, customizable dashboards, monitoring of blacklisted traffic, VPN tunnels and opened connections, and you've found yourself a top-notch component. The summary on each component should be clear, easy to read and understand, and detailed enough to help pinpoint subtle changes. It should also provide both connectivity diagrams and information on the status of hardware.

5. Reporting, log browsing, web portal

Reports are an essential tool in security management, providing easy-to-read and understand assessments of all security activity on your network. Reports are not only vital for internal use, but are also often required externally for use by public authorities and customers. Reports are a must when it comes to troubleshooting and security policy enforcement, noting trends that can assist with network planning and providing historical information that can help with analysis while investigating and recovering from an attack.

Log browsing is just as vital. A log browsing tool allows you to rapidly locate specific information you need to extract from a wide array of logs. Such a tool is essential to glean information that can help you detect intruders, pinpoint or recover from an attack, and troubleshoot problems. The most efficient log browsing tools include filtering capabilities, quick graphical statistics, and live monitoring of the case progress of any incident under scrutiny.

Access to specific logs may be necessary for your remote offices or customers, and secure web portals can provide just that without opening up your entire management server to outside entities.

6. Security policies and audit

Maintaining security policies is just as vital as creating them in the first place, and the most effective systems will allow safe and efficient maintenance using either a firewall or IPS sensor policy. For a system that goes beyond the norm, look for a solution that offers help creating, enforcing, distributing, and maintaining your policies. This can be done through the use of templates, sub-rules, and aliases as well as automation to prevent policy duplication and decrease the risk of human error.

Audits are a necessary component of a network, and your security management center should be capable of providing necessary information rapidly in an easy-to-understand format. The most effective systems include audit logs that store information to provide various ways to track and generate reports.

7. Incident management and alert escalation

If suspicious activity does occur in your network, the most effective security will alert you immediately so you can quickly begin investigation. Not only should you be alerted, but you should be given detailed information regarding the incident so you may best correct it. The ability to track your correction methods in journal form can assist with the process immensely, as can the ability to define alerts based on several criteria. These can include the time of day, type, originator, and severity of the alert.

8. Role-based administration access

Administrator access control can be a challenge unless you opt for a system that simplifies the process. This can be done by assigning different roles to different groups of administrators. Admins may have one role or several based on their privileges within the corporation. Once assigned to a role, admins enjoy the type of access that comes with that particular role.

9. High availability

Security system failures should not be an option within your network, and with the proper safeguards in place, they won't be. An automatically synchronized backup management server is a must to create a resilient management infrastructure that ensures continuous access to both your management and log server resources. Look for a solution that supports more than one backup server, allows active log servers to back up each other, and provides incremental database replication.

10. Remote upgrade

Upgrades are crucial to ensure your network enjoys the latest and most essential security measures. It is not necessary, however, for upgrades to be tedious, time consuming, or even difficult. The most effective security management systems allow for remote upgrades that save you time and tedium with a simple downloadable upgrade image that can be pushed to remote security engines using the management interface. That's it. The security engine should be immediately ready for action following the upgrade,

which you can complete in one simple step. An additional benefit of an effective remote upgrade allows the existing configuration information to be preserved and the ability to upgrade at any time.

Upgrading during business hours should definitely be an option, with an upgrade performed so seamlessly and quickly there is absolutely noimpact to end-users. This is typically possible through cluster nodes being upgraded one at a time, allowing the remaining nodes to handle traffic as each is rebooted. If for some reason a reboot fails, the upgrade should include a fail-safe function that allows it to roll back to the previous version. That means upgrades are either successful or they fall back gracefully, with no interruption of service in either event. One more important feature is the ability to schedule your upgrades at a later time, even if you upload new software during business hours.

Chapter 2

Ten Tips for Implementing Next Gen Firewalls Securely

Next generation firewalls are traditional stateful packet inspection firewalls with added functionality. They typically include integrated intrusion prevention, anomaly detection, and deep packet inspection that can identify application traffic and users, and may also include antivirus protection. Next generation firewalls should provide these added controls and visibility with the high performance through-put required by large enterprises. Significant performance degradation or loss of security controls as new services are turned up should not be an issue.

When evaluating your enterprise's next generation firewall purchase, here are some issues to keep in mind:

1. Architecture and domains

Intrusion prevention is one of the most vital capabilities for next generation firewalls, although some big name contenders are still leaving it out of their firewall mix. An intrusion prevention system works similar to an intrusion detection system, but it goes much further than simply alerting you to a potential threat and creating a log alert. Rather, a strong intrusion prevention system is proactive – it actively and automatically blocks current threats based on policies you have set.

2. Denial of service detection

Although it's crucial to block malicious traffic, you still need your good traffic to pass inspected, which is where more precise blocking comes in. Next generation firewalls must include the acute ability to fine-tune your rules to support either homegrown or off-the-shelf applications that your enterprise relies on.

You can set an IPS to block only specific packets when a threat is detected while the rest of the traffic and system continues to function without interruption. The most advanced – and effective – intrusion prevention systems will not only inspect specific packets, but will also pay attention to variations in traffic patterns and other activity that could signal a threat. This is done by building a baseline of acceptable behavior by application and by content inspection, with a strong anomaly detection capability adding to your enterprise telemetry.

3. SSL inspection

Deep packet inspection is also essential in your next generation firewall. Your enterprise's defense in depth strategy should always be a security priority. Malicious payloads may still be able to pass through despite the most rigorous controls. Deep packet inspection looks for malware and advanced evasion techniques (AETs) that can use multiple layers of evasions to conceal exploits that are targeted at SSL and other net-work security protocols. Encryption can be used to obfuscate malicious payloads. Remote access VPN can be the delivery mechanism.

4. Contextual awareness

Firewalls that offer contextual awareness provide critical visibility and adaptability to enhance your enterprise's security posture. Being contextually aware means the firewall can pinpoint the actual type of net-work traffic it is receiving, whether it is a YouTube video, salesforce.com, or a music download. Contextual awareness can also include GeoIP location awareness to track access and attempted access in the event of a security incident response scenario.

5. Full-stack and full-stream traffic normalization

Stalwart anti-evasion measures aimed against advanced evasion techniques (AETs) are another aspect too many technology leaders are ignoring when it comes to designing their requirements for a next generation firewall solution. As network traffic transits the network from source to destination, that traffic is split up into packets and given a sequence number. These packets can be out of order, allowing an AET to take over before they are reassembled in the correct order. Traffic normalization assesses the traffic sequence and looks for dangerous content before final delivery to the destination. Traditional security controls only check each protocol layer independent of associated layers and do not normalize the traffic sequence in order to investigate packet payload for malicious traffic. It is a laborious and expensive effort and often avoided by vendors at the expense of your enterprise.

6. Visibility features

While contextual awareness can help pinpoint the details of your traffic, those details are not particularly useful unless you have an organized way of looking at them.

Most security professionals that actively monitor network activity laud visibility features for dramatically increasing the overall functionality of the next generation firewall. These features let admins see for themselves, by role, what is going on in their network, rather than having to rely on additional devices or even other vendors to fill them in. It is all about telemetry and being proactive about situational awareness.

7. Comprehensive management consoles

The user interface and manageability of your firewall can make understanding and using it simple – or a nightmare. The most effective next generation firewall management consoles should come with several features aimed at quickly helping admins see what is happening.

Great user interfaces and comprehensive management consoles should give you a rundown, at a glance, of what is happening on your firewall and your other integrated and common network security devices. That means you need to see the top applications and their sources, countries, and destination hosts using GeoIP.

What you are able to view at the management console is also important. A management console should provide a look at IPS rules, different data types, URLs, and configurable views into categories that

admins expect for integration with other network and security management products.

8. Conversion adaptability

The ability to convert your existing firewall policies so they work with your next generation firewall is critical. For instance, a common problem occurs when converting a policy into a new firewall that only supports a single security zone in a single rule. Making sure the rules match what you need is a must, and so is selecting a next generation firewall that is as adaptable as it is reliable.

Also, don't fall into the trap of having thousands of rules that can overlap, be incorrectly written, and have not had an audit in years. The best scenario is to streamline your rules during quarterly reviews and with rigorous security testing.

9. Speed

Speed matters more than ever with the next generation firewalls when it comes to security and overall effective functionality. But speed kills if the proper traffic normalization is not done across all layers. Next generation firewalls can perform upwards of ten times faster than their ancestors, which is a major boon for forwarding traffic and an important component in evolving enterprise requirements.

An effective next generation firewall, however, needs speed and efficacy in another crucial area: when it comes to committing your changes to the firewall. Many firewalls operate by requiring the user to "commit" changes to the firewall before they go into effect.

It doesn't matter how rapidly you pinpoint changes if you're stuck with a delay before your firewall can commit and execute the changes. A lengthy commit delay can quell productivity when you are going for a succession of rapid changes and debugging processes.

10. Traffic control

Controlling ingress and egress traffic is a given when it comes to most firewalls. However, admins often attempt to use port number restrictions to control certain applications. A number of applications can easily adapt to running on the port specified for encrypted traffic if they need to, which can cause havoc with traffic control. Application specific, proprietary encryption can also be used to encrypt data; and random port hop can make it difficult to implement additional controls and countermeasures. Visibility and controls as well as effective counter-measures are more critical than ever across your next generation firewall because of these security challenges.

Chapter 3

Ten Tips for Implementing SSL VPN Securely

As workforces grow more mobile and geographically dispersed, SSL VPN is becoming integral as a means to achieve secure access to corporate resources wherever you are, whenever you want. The benefits of SSL VPN, technically known as Secure Sockets Layer Virtual Private Network, are immense.

In addition to offering you and other trusted company associates easy access to your network, SSL VPN works from any standard web browser and does not require the end user to install any type of specialized software. This type of set-up is especially useful for companies with several mobile users who need to connect from various locations. Security is a top priority with SSL VPN, and you can ensure secure access with help from these ten tips:

1. Virtual appliance

Utilizing a virtual appliance allows an application portal to be built in accordance to your needs. The appliance can be dynamically populated based on your criteria and serve as an integral safeguard for connections. An effective virtual appliance has a heavy focus on strong authentication, end-point security, assessment, and trace removal techniques. It also allows for immediate deployment of the desired connection as well as easy building of application portals.

2. Access control and auditing

Controlling the degree of access end users have to corporate resources is a must for a secure network, as are auditing capabilities. Access control capabilities need to be granular and flexible, offering or denying access based on any combination of your chosen parameters. Admins should have the option of setting up unique access control characteristics for each application individually, with the additional benefit of re-usable rules to maximize efficiency.

Auditing is a vital characteristic of any network to ensure strict corporate, industry, and government compliance regulations are always being met. The most successful auditing options include detailed reports as well as various means of performing an audit, be it comprehensive or consolidated. A major plus for auditing capabilities is finding a system that guarantees compliance regulations right out of the box with no amendments or adjustments necessary.

3. Authentication

Authentication is a must with any network, and the greatest challenge typically is to provide something that maximizes both security and ease of use. Authentication options should provide several choices that best suit the needs of each device and user. Choices may include passwords, mobile ID, or even more challenging options. The most effective authentication provides a dozen or more options, ranging from the most basic to the most sophisticated, any of which are easily integrated into the existing system. One

best practice to consider is chaining the authentication methods to provide a holistically stronger, multifactor process without being too intrusive. For example, the user would enter a name and password, a digital certificate would be generated, and then a one-time password delivered to the user's mobile phone to complete the authentication.

4. End-point integrity

Not just any device should be allowed access via your SSL VPN, lest the device be compromised and used as a steppingstone for entry into your valued corporate resources. The most secure SSL VPN thoroughly inspects each device for specific requirements. Those requirements may include anti-virus software and firewall, the operating system and patches, spyware, network configuration, hardware assessment, and a review of the device type. Those devices that do not meet the requirements may be denied access altogether, or you may choose to have the users forwarded to an updated site or granted limited access as needed. End-point integrity also ensures your corporate security standards and guidelines as well as any compliance regulations are always being met. Finally, you should make sure you can validate the end-point security during the entire session, not just at the beginning. You don't want a valid session to start and then become compromised.

5. High availability

Failed connections that are supposed to work are another stumbling block that can arise with SSL VPN. One of the most effective ways to defend against this is through fault-tolerant authenticated sessions that allow two appliances to form a mirrored access-point pair. If one access point does happen to fail, another node immediately takes care of corporate application access, providing truly available access. Even when the initial access point is functioning up to par, the additional access point can be placed in a different geographical location. This provides an automatic safeguard and a tool that meets disaster recovery requirements.

6. Integration and management

Easy integration and management of your SSL VPN is another way to help keep it highly secure. Integration in the most effective systems typically consists of the ability to add accessible applications to your application portal. You should have the capability to define how each application is presented and further define users who may access each application and when.

The management end of your SSL VPN should function just as seamlessly, with a clear and user-friendly interface. Such an interface should ensure comprehensive security of your networks while you easily administer and maintain remote access to the system. The interface should allow you to consistently monitor and manage the system, report network incidents, and manage resource access as well as accounts and storage from one consolidated interface.

7. Proxy access

Although end users will access your corporate resources upon your approval, the most secure SSL VPNs will not allow them to access the resources directly. All traffic should instead be routed via a web proxy, which accesses the back end applications and then delivers the information back to the end user. The proxy mechanism should allow end users to access web applications as well as client-server applications, terminal applications, and file server applications. Based on an advanced link translation engine, the proxy mechanism is a major safe-guard to your network by setting up a buffer between the end user and your valuable corporate resources.

8. Single sign-on

Single sign-on is an optimum benefit for end users, requiring only a single authentication to access all the resources to which they are granted access. Rather than facing re-authentication, multiple passwords, and a series of potentially frustrating stonewalls during sessions, a single sign-on takes care of it all in one swift and efficient move. Single sign-on capabilities are not only useful for user ease and security, but can also cut costs by offering a single digital identity to access multiple departments or businesses if engaged in mergers or business-to-business partnerships. A single sign-on that can combine with Federation ID provides maximum flexibility, so seek a sign-on that provides such capabilities.

9. Trace removal

Maximum security for your SSL VPN must come with trace removal, an option that plays a heavy role in devices accessing resources from insecure locations. This applies to many Internet cafés, airports, hotels, access points outside corporate security boundaries, and other untrusted areas. Trace removal eradicates the trail of information that can accumulate during an access session, such as URL history, registry entries, downloadable components and files, cached pages, and cookies. The most effective trace removal options will allow you to customize the rules and offer the choice of including temporary files. If your network contains a large number of roaming users, trace removal is vital to the security of your network.

10. User interface and universal device support

A highly effective and secure system will offer a user interface that is easy to comprehend and use as well as one that provides universal device support. The application portal should be intuitive, offering the end user clearly understood options and menus listing all applications available to them. Guesswork and confusion are never beneficial for the security and use of a network, and a user-friendly interface takes care of both. The user interface should automatically adapt to fit whatever device it’s being accessed from, whether it’s a laptop, netbook, PDA, or mobile phone.

The universal device support should also extend to any device that can access a web browser. Rather than requiring specialized hardware, software installation, or specific parameters that can make or break your SSL VPN access, access should work on the wide range of devices found in today’s workforce with the same secure and easy access your business requires to succeed.

Chapter 4

Ten Tips for Implementing Virtualization Securely

Virtualization has been going strong more than half a decade, and it's not expected to slow down anytime soon. In fact, an International Data Corporation study predicted that 70 percent of all new-shipment server workloads will be based on virtual machines in a mere two years. Just because virtualization is popular, however, does not mean it's always securely implemented.

Some firms may try to cut corners on cost when they implement effective virtual security technologies, while others may not fully comprehend the concept, which limits their ability to provide proper protection for their infrastructures. Virtualization has its specific challenges, but those challenges can be successfully met. The following ten tips can help you implement virtualization securely so you can realize the full scope of benefits that come with this highly efficient and cost-effective technological trend:

1. Understand the concept

Understanding what virtualization is all about is key to implementing it securely. The term refers to creating a virtual version of a computing device, resource, application, or even multiple operating systems on a single server. Rather than implementing multiple servers for all your needs, a single server can become the base of all your operations. Each system, application, or resource runs independently on this single server as if it was, in fact, set up individually and wholly autonomous.

2. Know the benefits

You can immediately assess the major benefits of virtualization, with cost effectiveness topping the list. You no longer have to invest in multiple servers or other costly hardware when all your needs are met on a single device. Your costs for deployment, management, and maintenance also decrease substantially.

Managing a virtual environment becomes much less difficult when your systems, applications, and other functions are controlled and dispatched from a single location. Managing the security of the virtual environment can also be infinitely easier than employing security tactics for multiple servers and physical devices.

The most effective virtual environments will allow you to utilize a single connection for multiple IPS, employ scalable VPNs, and ensure true high availability regardless of any single point of failure. That means customers can complete transactions, suppliers can remain connected, and information can maintain a steady flow during maintenance, system overload, excessively heavy traffic, equipment loss, or a targeted attack.

3. Realize the challenges

While virtualization comes with a myriad of benefits, it also has its share of challenges. Understanding

these challenges can help you learn how to meet them successfully. Your first concern with security is being aware of applications that may not function properly, or at all, in a virtual environment.

Traditional firewalls are a prime example, as they rely on highly specialized ASIC-based hardware to run and will not function on a virtual machine. The same holds true for a traditional IPS. The traditional forms of protection typically protect the main server from incoming traffic but offer no protection between virtual machines. Obtain protection between the VMs and you've effectively met a major challenge.

4. Beware of virtual LAN (VLAN) tagging limitations

Virtual Local Area Networks, or VLANs, divide different departments into various zones where they are free to connect within that zone, the same way routers work for traditional LANs. Each VLAN requires tagging for optimum security, with each VLAN enjoying its own unique set of policies for acceptable use. Anyone who goes about manually setting, maintaining, and updating these policies is going to face a tedious and time consuming task, especially when hundreds of VLANs may be in use from a single server. Manual updates also often require reconfiguration and pose a security risk, providing a window of opportunity for malicious infiltration. In other words, manual updates are not a good choice.

5. Avoid falling prey to retrofitted virtual environments

Some may believe using hardware retrofitted for virtual environments can be a fast and easy solution to security for their virtual infrastructure. It's not. Not only does adding layers of physical appliances to a virtual environment counter the very purpose of virtualization, it also creates severe security risks.

Attempting to implement traditional firewall and IPS application between virtual hosts increases the complexity, decreases the efficiency, and hurls the door wide open for security breaches. The outside security devices are also unable to capture and deliver the comprehensive visibility you receive from solutions that reside within the virtual environment.

6. Steer clear of single point virtual security products and virtual switches

Single point virtual security products may be effective for monitoring what's inside the virtual environment, but that's as far as their capabilities go. They are unable to see what's happening in the rest of the infrastructure, which may be a combination of both virtual and physical environments. This creates double work for admins as they must then log in to two different systems to properly monitor them.

Virtual switches are just as ineffective a solution for a virtual environment. They are limited to providing only layer 2 and 3 security, wholly ignoring application layer security or IPS capabilities. They are also limited in the amount of visibility they provide, which is typically only what the admin can see through a management console. Admins are blind to activities through their networks, which can be a surefire formula for a security disaster.

7. Embrace software-based virtual security appliances

Virtual security appliances work in a virtual environment by implementing security functions using software. This software can be run on top of or even as part of an operating system without the need for purpose-built ASICS that can be ineffective in a virtual environment. The security appliances should have the same next generation functionality as top-notch physical devices but in the form of an easy-to-implement virtual machine. Hardware-based products are blind to the virtual environment while software-based appliances allow you to keep a keen eye on all activity.

8. Invest in a stalwart virtual firewall

A virtual firewall provides effective protection for and a comprehensive view of a virtual environment that a traditional firewall can't. The most effective comes as a ready-made, easy-to-add appliance that can be managed through a unified management center from which you also manage your traditional appliances. Virtual firewalls should also provide granular access control, intrusion prevention for both web and VoIP traffic, content inspection, and the ability to provide both stateful inspection and application-level protection, based on the methods best suited for your environment. Multiple alert methods, auto-updates, and comprehensive logging and easy filtering are other features to look for.

9. Choose an effective virtual IPS Avoid falling prey to retrofitted virtual environments

Similar to an effective virtual firewall, your virtual IPS should be ready made, easy to add, and managed through a unified management center. It should also offer the same type of multiple alert methods and comprehensive view of your network. The most effective virtual IPS will utilize multiple analysis techniques to protect your virtual hosts from network attacks while detecting and preventing a wide range of network traffic abuse. Other useful features include flexible deployment options that can work in physical and virtual environments in both inline IPS and IDS modes without requiring topology changes.

10. Protect with an SSL VPN virtual appliance

One more vital component in your protection should come from an SSL VPN virtual appliance. This Secure Socket Layer virtual private network appliance should harbor virtualization technologies that allow the implementation of virtual datacenters where they're needed most. This could be at a server consolidation point or a point where a hypervisor is distributed across multiple physical servers.

Such an appliance helps ensure hardware failures do not create systems failures while supporting optimized network drivers for peak efficiency and performance. Additional features of your SSL VPN virtual appliance should include rapid deployment into the infrastructure and a native virtual appliance format.

A major benefit is keeping your operating and maintenance costs at a minimum, but it also has several other advantages. It allows for the easy building of secure, authenticated application portals for corporate resource access. The virtual appliance native format will also allow for immediate deployment, effectively reducing your TCO/TCA.

Chapter 5

Ten Tips for Implementing Next Generation Security

Network security is in dire need of a jumpstart. The misalignment between threat and threat mitigation is severe. CIOs must have a prioritized roadmap for upgrading their network security infrastructure to combat these threats, and a thorough understanding of their risk tolerance at different points in their network. From there, companies can map out the processes, actions, and insights they will need to future-proof their security posturing and minimize risks.

Network security looks a lot like it did a decade ago. It's hardware-based, difficult to configure and manage, less than dynamic, and lacking in visibility. It's misaligned with the current corporate and consumer environment that has entered a new generation of information sharing. Even more alarming is that it's failing to keep up with a new generation of network security threats that include advanced persistent threats (APTs), advanced evasion techniques (AETs), and organized cybercrime.

The pressure to modernize network security and establish alignment between risk and protection is on. But that doesn't mean the roadmap is clear. Ripping and replacing an outdated network security infrastructure is not an option for most companies. The migration to next generation security will be a process, but one that can be expedited with the right foresight and guidance.

To help you navigate the path to next generation security, here is a checklist of issues to consider.

1. Do you know what devices/systems are accessing your network?

Expansive networks, IT ecosystems, and bring-your-own-device (BYOD) have made it difficult to track exactly who's accessing your network and from which device and system. You should maintain an asset inventory of all systems connected to the network and the network devices with access authorization.

2. Do you have continuous, real-time monitoring?

Take a cue from the U.S. government and make continuous monitoring a mandate – not an option. The ability to identify threats before they strike is only made possible by real-time network monitoring.

3. Are you ready for IPv6?

Today's enterprise networks need to support IPv4 and IPv6 traffic. However, securing IPv6 traffic has presented a few challenges. Despite vendor claims, most vendor firewall and next generation firewall (NGFW) devices can't handle realistic volumes of IPv6 traffic. They either compromise security or compromise network performance – neither of which is acceptable to your business. Make sure vendor claims regarding IPv6 performance have been independently verified.

4. Did you segment the network?

Non-disruptive network segmentation is key in obscuring the path to a data breach. The parts of the network that contain the most sensitive information should not be easy to reach. At each critical junction in your network security plan, there should be physical and logical controls to make it difficult to reach sensitive information.

5. Do you use multi-factor authentication for remote access to the cloud?

Having a simple password to protect sensitive information is insufficient – especially when accessing cloud-based data. Implementing multi-factor authentication means greater protection for all business stakeholders. Furthermore, multi-factor authentication must be ergonomic – that is, easy to use and deploy.

6. What about outsourcing?

Companies have previously held security close to their vests – and with good reason. However, as IT becomes more and more outsourced thanks to the cloud, network security has become more disparate and difficult to manage. Many enterprises are turning to managed security service providers (MSSPs) for assistance. Today's CIOs – even those who have taken a hard stance against outsourced security in the past – need to revisit this debate. How many resources are needed to maintain the enterprise's security posture today and what will be needed in the future? What should be insourced and what can be outsourced to keep IT focused on innovation?

7. Have you optimized and centralized network security management?

This is perhaps the most crucial part of next generation threat protection. Visibility and the ability to quickly act when a threat is detected can mean the difference between protection and a destructive data breach. Having a way to centrally manage, update, and configure all of your network security devices is not a nice "to-have"; it's a must-have in today's complex network environment.

8. Have you aligned your security and business needs?

Does your security policy match the needs of your business? Sometimes security can take itself too seriously and restrict growth, innovation, and new means of improving productivity. Communicating up and down the management chain helps everyone understand the importance of security while giving you a view into business needs and drivers.

9. Are you compliant?

It's expensive to achieve compliance, but it's more expensive to fail an audit. And since requirements constantly change, you have to stay on top of all processes and reporting requirements. HIPAA, GLB,

Sarbanes-Oxley, and PCI are not going away. Expect new compliance measures as well, particularly related to cyber terrorism.

10. What about the future?

Your business changes. Your network changes. And the threat landscape changes. The question is – can your network security infrastructure adapt easily and cost effectively? Today's businesses need scalable, flexible security solutions that can be easily updated, expanded, and contracted depending on demand. This should be a critical part of any company's network management strategy.

Chapter 6

Ten Tips for Implementing IPS Securely

An intrusion prevention system (IPS) includes all the features of an intrusion detection system (IDS), but it also has the ability to act upon malicious traffic. The IPS usually sits in line with network traffic so it can quickly shut down attacks, typically by blocking access from the attacker or blocking access to the target. In some cases, the IPS can talk to the firewall to block an attack.

Implementing IPS security effectively requires paying attention to ten vital issues that every IPS needs to address to help ensure your network is the safest it can be:

1. IDS, IPS and hybrid modes

Your IPS should be multifunctional so that you can deploy it depending on your exact need.

In the IDS mode, the device is passively monitoring network traffic. The IDS mode can be used for aggregating network traffic from multiple VLANs or physical traffic sources, such as switches and wiretaps, into one centralized IDS sensor or IDS cluster. The IDS is able to restrict traffic by sending resets or requesting a firewall or inline IPS to isolate the segment from other networks using blacklisting. The IDS mode works well when you have to protect large local area network (LAN) segments.

In the IPS mode, the device is configured inline between the network traffic paths. The inline sensor should be able to inspect one to four physical segments simultaneously or more if VLAN tagging is used. The IPS should be able to block traffic or send requests for a firewall or other inline IPS to isolate the segment from other networks using blacklisting. The IPS mode is also effective in blocking attacks if you can identify a clear threat path – for example, traffic from the Internet to a DMZ segment, or traffic from an internal network to the Internet.

In the hybrid mode, the same device is configured to function in both modes. Using the same device in both modes is an efficient and cost-effective solution for smaller implementations.

2. AET Protection

Advanced evasion techniques are real and are currently used by NSS Labs and other organizations to test security vendor products. In its latest report, Verizon stated that in 31 percent of attacks against large organizations, an attack vector remained unknown.

Analyzing AETs requires that the data streams are 100 percent inspected and normalized, but 95 percent of organizations are not doing that. Most current security devices cannot flag or log AETs separately. At best, they may report on anomalies or suspicious traffic.

Also, it's important not to confuse an exploit with the method. Stuxnet becomes visible when it hits the target; it stays there and is easy to investigate once the code is isolated and recognized. AETs can be analyzed if your IPS records analyze ALL traffic, not just what is logged by the security devices. Ask your

IPS vendor what their strategy is for dealing with AETs. And download the free Evader testing tool for your lab at http://evader.stonesoft.com.

3. Event correlation

Make sure your IPS uses event correlation to reduce false positive events and provide accurate protection for network services and intranet users.

Event correlation looks at log data from one or more sensor engines, searching for malicious event sequences, preferably in real-time. Event compression cleans repeating log events and minimizes the bandwidth requirements from remote offices back to the data center. A good event correlation engine can alert the IPS to isolate an attacker or network worm on all firewall and IPS engines simultaneously, minimizing the damage to network services and clients.

4. Web filtering

A great enhancement for your IPS is web filtering, giving you multiple benefits such as increased security by preventing access to known malware and phishing sites, as well as improved work efficiency and bandwidth usage by blocking access to unwanted websites.

Advanced web filtering systems can offer plenty of options, such as blacklists and white lists where you can set rules for the entire network. Customizable options are a major plus in letting you pick and choose exceptions to the rules. You should also be able to produce reports of web browsing habits and activities.

5. SSL inspection

SSL inspection is vital in ensuring that no attacks, viruses, or other unwanted content can enter or exit the organization network by disguising itself inside the encrypted HTTPS channel. SSL inspection gives network security administrators an ability to monitor traffic inside the TLS/SSL encryption and to detect and react to any unwanted content. Your IPS should have a controlled way to open the encryption in the network and to submit the encrypted traffic for the same inspection as the clear-text HTTP data, eliminating this important blind spot in network protection. In addition, SSL inspection is important for meeting the PCI DSS requirements.

6. Denial of Service protection

Your IPS should provide protection against illegal input and traffic flood DoS (Denial of Service) attacks without disturbing legitimate network traffic. Connection flood or web service starvation attacks are typical examples of Distributed DoS (DDoS) attacks. TCP SYN flood attacks are stopped by blocking the incoming connection attempts from spoofed address sources under an attack and preventing them from reaching the target system. Your IPS must quickly identify the spoofed connection sources and block them, while allowing valid user connections to pass through. UDP flood DoS attacks are controlled by rate limiting the incoming UDP datagrams against the protected web service.

By using correlation techniques in detecting suspicious behavioral patterns in web service communication when the botnet host has been identified, the IPS blocks the malicious host communication for the web service.

7. Central management capabilities

Central management is essential for IPS security since it allows you to manipulate your system without having to manually touch every single remote location to make a change. Central management typically lets you monitor and manage appliances and components with options that may include alerts, security content updates, appliance updates, firewall, and intrusion prevention settings. The result is less administrative time devoted to network security, incident, and log management operations and the integration with other security components to enforce immediate threat mitigation policies or software updates.

8. Performance

Your IPS could affect your network if it is not implemented properly or if the IPS product is poorly architected. Look for the ability to use clustering to share processing connections, thus enhancing performance and reducing downtime.

The deployment of the components of your IPS could also minimize the risk of performance degradation. The IPS has to capture and analyze traffic, so it is best to separate the analysis component onto a dedicated system. Ask your IPS vendor how to best deploy your IPS with the least impact on your network performance. Also, ask about how signatures and other context information are analyzed to see if performance is an issue.

9. IPv6 ready

Major operating systems and core networking components offer IPv6 support. For example, Windows Vista uses IPv6 addresses by default, which may be a security threat without properly implemented access control and deep inspection. In addition, malicious traffic may be hidden inside IPv6 and IP-in-IP tunnels, which many security solutions still fail to protect.

Make sure your IPS provides stateful access control and full deep inspection capabilities for IPv6 network traffic, including IPv6 encapsulation, IP-in-IP, and GRE tunneling protocols.

10. Integration with your firewall

The essence of a next-generation firewall is the ability to interact with an intrusion prevention system. The integration of these capabilities can be either within a single system or separate, but beware of issues that can arise around reporting, throughput, and management.

Chapter 7

Ten Tips for Implementing IPv6 Securely

Many organizations are being misled about the complexities surrounding IPv6 security. They don't believe there's much difference between securing IPv6 traffic and IPv4 – but that's not true. This misperception is compounded by the fact that organizations aren't sure what needs to be done when, and that vendors are making false claims about how well their products perform in an IPv6-ready network. The following tips should help you weed through the hype surrounding IPv6 security and prioritize your security initiatives in a cost-effective manner:

1. Revamp your existing network

Revamping your IPv4 network involves cleaning up, throwing out, and upgrading to new. Clean up and kick out outmoded and outdated features by ensuring every aspect of your network that can be effectively upgraded to the next level is, in fact, happily humming along at that level. Starting with a clean, uncluttered slate makes it much easier – and safer – to implement IPv6 without a ton of hassle and future problems.

2. Plan a gradual introduction

Take a cue from the Social Security Administration, which has been working with IPv6 for more than half a decade already. The full implementation is planned for three stages over a span of another six years. You do not have to tread as slowly as the government, but gradually introducing IPv6 gives you plenty of time to ensure IPv6 is going to function with your now state-of-the-art IPv4 infrastructure. It also keeps your budget in check.

3. Choose dual stack

Opt for dual stack mode for your IPv6 implementation. Dual stack comes with a host of benefits, although it may require router upgrades to meet the memory and power demands to support running both IPv4 and IPv6 simultaneously. In addition to being straightforward to implement, the dual stack approach allows your system to support applications that are not yet functional with IPv6. It can also help eliminate the need for tunnels, which are already being viewed as a veritable breeding ground for security issues.

4. Take care of your tunnels

The National Institute of Standards and Technology's "Guidelines for the Secure Deployment of IPv6" suggests viewing and treating tunnels the same way you would an external link: with extreme caution. It recommends inspecting every single shard of tunnel traffic before you permit it to either enter or exit your system. This inspection consists of reviewing all IPv6 traffic, including those within the IPv4 packets, with

the same scrutiny and systematic examination you give to all your traffic. Suggested tools include the usual gamut of virus protection, intrusion detection, network ingress filtering, packet filters, and application proxies. Further, fortify the tunnel endpoints with even more stalwart security measures, such as authentication.

5. Mind the malicious

Malicious users are already infiltrating IPv6 quicker than they have hit other advancements. Do not forget the warnings about the dangers of router advertisements and man-in-the-middle attacks. Some attacks can delve deep into your network before you even realize anything is amiss, making them more destructive than ever. These and similar attacks are coming from scripts that are almost too easy to use. Memorizing every type of attack and the solution to go with it would be impossible. Being aware that many already exist and many more are sure to come is crucial.

6. Upgrade to a certified firewall

Be careful about claims concerning IPv6 readiness. Without outside verification, it is likely the vendor may have simply pointed a traffic generator at their product and claimed it works. You must look at products that have undergone third-party certification. This certification applies hands-on testing using publicly accepted evaluation methods to assure you know exactly what your firewall can handle.

7. Require authentication

Authentication is more critical and, fortunately, easier than ever before. You should look into an HTTP/HTTPS proxy for users to access the Internet. Once you set up required authentication to even get online, you have reduced the threat of unwanted parties entering your system without your approval.

8. Hit the books

Know IPv6 syntax. The syntax is very similar to that used with IPv4, but with notable differences in the foundation. Knowing the syntax makes it much easier to quickly know how to deal with a security breach or implement necessary measures. Since IPv6 has technically been around for more than a decade, there is no shortage of information on the subject from several technology giants – as well as a 188-page guide from the U.S. government.

9. Hit the “off” button

Shutting off IPv6 capabilities when you are not using them may sound like a no-brainer, but it may not be as straightforward as you think. That’s because a number of programs have already been configured to work with IPv6, and just as many may already have the protocol turned on automatically by default. Check, double check, and triple check your environment to ensure IPv6 is only enabled when it’s actually being used. Deploying a mechanism with the ability to disable IPv6 in bulk may be a wise investment.

10. Know how to kill

Even with large portions of your network disabled for IPv6, you can still face the threat of unwanted IPv6 visitors. When that becomes the case, you need to know how to kill it before it can infect others associated with your network. This is where knowing IPv6 syntax can be a lifesaver, particularly for setting up effective firewalls and traffic filters. You can create filters that let in what you want, keep out what you don’t, and help to ensure when you’re up and running with IPv6 that you are actually up and running.

Chapter 8

Ten Tips for Implementing BYOD Securely

As Bring Your Own Device (BYOD) quickly migrates from a corporate trend to the accepted norm, you need to better understand how BYOD will impact all aspects of your network security strategy.

BYOD is another technology trend that moves a company from a position of risk avoidance to risk management. Many IT organizations get it wrong by focusing on only one piece of the puzzle – such as the device. If organizations want to minimize the risks of BYOD, they need to assess the impact on the network security ecosystem and understand the big and small weaknesses it creates.

Here are ten tips for implementing BYOD securely and effectively within your enterprise, while fostering secure, remote access to business critical information:

1. Go beyond passwords to authentication

Static passwords, combined with the risks of BYOD, are not enough to ensure secure remote access to sensitive business data and systems. Companies should consider multi-factor authentication methods to strengthen security while continuing to prioritize usability. One-time passwords and alternate notification methods (e.g. text messages) are two ways to make the authentication process holistically stronger.

2. Secure remote access with SSL-based VPN

Once you have authenticated a user, companies must secure the network connection. SSL VPN gives employees enormous flexibility to access the network securely from any location and from any mobile device. Furthermore, unlike IPSec (Internet Protocol Security), SSL VPN provides secure remote connectivity without the need for software to be installed on each device.

3. SSO for password fatigue

Separate logins for individual applications are both a hassle and a security risk, as users may deploy insecure methods for keeping up with different passwords. Single sign on (SSO) tools let employees use a single password to access a portal of company and cloud applications. They can be part of an SSL VPN configuration.

4. End node control

Once an employee leaves the company, network access should leave right along with them. However, that is not always the case unless there is a way to instantly and effectively block specific users. Find a solution that manages devices from the corporate side, not just the employee side, and that allows you to

quickly remove a specific user's access privileges with a few keystrokes. This should be accomplished without requiring redefinition of the entire user base, which is both time-consuming and prone to error.

5. Applying a Federated ID

Federated ID simply means that the person's identity is stored across multiple systems, such as when you use Facebook or Twitter to log in to another account online. The same works for your organization, where you authenticate a user and then allow him or her access across internal and external systems that you manage. Federated IDs allow single sign-on for the employee. What are the benefits? The employee logs in to any approved system easily, the corporation controls access even to cloud-based applications, and the service provider does not need to maintain user profiles.

6. Soft tokens with BYOD

Physical security devices have become risky and cumbersome. BYOD represents a wonderful opportunity for enterprises to save money on the costs of buying, managing, and distributing hard tokens or other physical devices. Soft security tokens that interact with an employee device, such as a smart phone, provide an ergonomic solution that works for both parties, and can be easily updated and managed as the threat landscape changes.

7. Manage the entire process

The risks of BYOD make it even more critical to have a centralized view of network activity, incoming threats, and abnormalities within the network, as well as the ability to quickly and easily respond. It is important to find a centralized management console that provides comprehensive reporting, incident process management, progressive multi-channel alerting, geotagged statistics, and the ability to apply governance across the entire platform.

8. Appoint a leader, execute a strategy

Management of a BYOD strategy should not be a responsibility that's lumped in with the hundreds of other tasks that IT manages. Appoint a cross-functional leader who will oversee the policies, guidelines, roles, and duties of the various departments that are involved with executing a BYOD strategy. This person will be responsible for determining every aspect of BYOD within the enterprise, including what devices will be allowed, what departments will support them and who will pay for sup-port, service, data plans, etc.

9. Implement a policy

No matter who owns a device, employees must abide by corporate security protocols if they're using that device for business. A BYOD policy should cover the basics like requiring an auto-locking capability and a personal identification number (PIN) as well as support encryption and remote wipe in case of theft. The

policy should also cover what types of data can and can't be stored on the device, what to do if it's stolen, and what are acceptable and unacceptable backup processes. Most importantly, having a written user agreement policy – and communicating it regularly – is critical in order to emphasize to employees the importance of following security procedures when using their devices.

10. Encourage common sense

Don't assume employees will use common sense – reinforce it by educating them. Regularly review even the most obvious mobile device security measures, like what to do if a device is lost or stolen, conducting regular device updates, locking devices when not in use, and using discretion with downloads.

Chapter 9

Ten Tips for Implementing AET Prevention Securely

One of the most worrisome and potentially crippling threats to next generation infrastructures is the advanced evasion technique, or AET. Stonesoft announced its discovery of AETs in October 2010 and has since continued to expand its research in the field of AETs with the aim of better understanding and mitigating the threat.

By December of 2010, Stonesoft had already produced a technical paper on AETs and announced the first details of 23 new evasion methods being implemented. By the RSA conference in February 2011, Stonesoft announced an additional 124 new evasion techniques it had uncovered. Since the discovery of AETs, Stonesoft has been developing and making available security measures to effectively thwart AETs.

“Our research indicates that the threat posed by advanced evasion techniques is more real and more dangerous than we initially believed,” said Richard Benigno, Stonesoft’s U.S. vice president. “While the lion’s share of the work needs to happen at the product R&D level, there are certainly things organizations can do today to better protect their networks from AETs.”

Keep in mind these ten things when testing your environment for vulnerability to AETs:

1. Understand the difference between AET and APT

AETs consist of any evasive hacking technique that allows an intruder to bypass security detection during a network-based attack. While AETs themselves are not malicious, they are the vehicle through which any number of malicious attacks can be successfully delivered to vulnerable network targets. They are typically successful in their infiltration due to their ability to ensure that traffic looks normal to security devices, which then allows traffic to pass freely.

These stealth cyber attack methods bypass network security, are stack-able through simultaneous execution on multiple protocol layers, and are capable of changing dynamically, even during the attack’s execution.

Advanced persistent threats, or APTs, generally refer to a group, such as a foreign government or hactivist party, that applies a number of techniques and attacks over a long period of time.

2. Understand why security measures are foiled

AETs foil security measures for two main reasons. One is the astronomical number of combinations AETs can employ. The other is the type of inspections many security devices employ. Those that perform packet or pseudo packet-based inspection across a limited number of protocols and network layers, using signature pattern matching, simply are not sufficient to stop the threat of AETs.

Additionally, no published device lab tests have satisfactorily tested device behaviors when they encounter AETs. Therefore, no acceptable comprehensive solution has been recommended.

3. Understand the importance of normalization

Traffic handling, inspection, and detection are three main weak points in a network. Traffic handling for many IPS devices is done with a throughput orientation, which does not allow for full normalization. Data traffic should be normalized 100 percent on every protocol layer before payload inspection is executed.

This is not typically the case for many devices, which are instead de-signed to optimize the inline throughput performance. Furthermore, the devices are optimized in a clean, or simulated, network that is never targeted with a complex attack that is difficult to detect.

Instead of performing full normalization, many devices implement shortcuts and therefore only perform partial normalization and inspection. A prime example is TCP segmentation handling, which is generally extremely limited and performed only in chosen ports or protocols. Shortcut exploitation by evasions becomes a strong possibility.

Rather than inspect only segments or pseudo-packets, proper security devices must inspect a constant data stream. This fundamental design flaw is not amended, especially with hardware-based products that would require a significant R&D outlay to redesign.

Data stream inspection also requires additional memory and CPU capacity to perform in throughput. Many vendors find such a change impossible, leaving networks highly vulnerable to evasions that exploit the limited inspection scope by spreading attacks over segments or pseudo-packet boundaries.

Detecting invasions through current network security devices is impossible when the devices rely on packet-oriented packet matching as their approach to exploitations. Because AETs can use so many combinations to infiltrate a system, a 100 percent pattern match for detection and blocking is required.

4. Know how powerful AETs can be

The vulnerability to AET infiltration is not simply a theory. While we generally lack reliable published lab test results, organizations have taken note of the tremendous risk AETs pose and have run their own series of tests through their own products as well as through other security devices.

In a Stonesoft test running 124 randomly selected AETs through the leading devices, the devices largely failed to detect AETs, with the results reported through the CERT-FI vulnerability coordination process flow.

ISACA reported on the AET testing results of leading firewalls, IDS, and IPS systems witnessed in Helsinki, Stonesoft's corporate head-quarters, and deemed some security appliances' performance "down-right useless when faced with these new style crafted threats." Results from intrusion attempts running 104 AETs reported 34 successful intrusions, compared to 17 blocked attempts. The testing was performed in approximately five seconds.

5. Watch what industry is saying about AETs

ISACA is not the only industry organization that has noted the extreme threat of AETs and what the non-

profit calls “the future of insecurity.” Gartner explored AETs in a lengthy research report, asking if the techniques merited mention as being advanced or if they should instead be thought of as an evolution. Other industry organizations have expressed both dismay and concern at AETs’ ability to infiltrate even the most seemingly secure networks and devices.

One noted network security consultancy organization deemed the AETs “a genuine threat, presenting a very real risk to your network.” This conclusion was drawn after Stonesoft performed AET testing on a demo network with a leading IPS, even with tuning and updates utilizing the most current patches. The organization additionally witnessed its own demo system fall prey to AETs and, as reported in a company article, “We are now hounding the vendor to provide a solution.”

6. Know what it takes to defeat AETs

Defeating AETs involves utilizing a data stream-based approach with layered protocol analysis. All data traffic must be recorded and analyzed with the utmost precision. The key to this precision is to analyze data as a normalized stream rather than as a packet or combination of packets. Doing this requires multiple parallel and sequential state machines through which the data stream is fed and all data traffic is analyzed by default.

The lower protocol layers must be examined, with the security device only passing slightly modified or non-modified TCP segments and IP fragments. Those that contain overlapping data or conflicting data are not passed through, resulting in an effective normalization. This process ensures network traffic passing through the IPS is interpreted and the data stream reconstructed for inspection and analysis in the upper layers.

It is essential the TCP layer is inspected as a reassembled data stream, rather than in segments. Assembling the data transmitted in a TCP connection into a data stream provides detection of attacks in the stream that individual segment inspection may miss if the attack stretches across TCP segment boundaries.

The higher protocol layer inspection must have the capability to inspect certain protocol elements in greater detail. This can be done by inspecting those elements as separate data streams and then normalizing them as per the protocol.

7. Realize the importance and benefits of centralized management

Centralized management is an essential factor in effectively protecting against AETs, mainly due to its ability to perform rapid system-wide updates and patches as necessary. It also offers a myriad of other benefits, such as decreasing the amount of time and increasing the ease of maintaining a secure network.

A centralized management system places network functions in one centralized location for viewing, monitoring, and amending. Administrators may enable appliances and monitor all network devices. They are also able to create and change parameters across more than one device throughout the network, eradicating the risk of human error and the potential difficulties of configuration. Most centralized systems

offer comprehensive reports, automatic updates, and reminders available in one enterprise-level location.

8. Test evasions in your own environment

Reviewing your hosts and servers is essential to ensure everything is up-to-date. Inspect your hosts to ensure they have the latest policy and the virus definitions for both the hosts and server. Examine the infrastructure for disconnected hosts, as they can pose another point of vulnerability.

Regularly monitoring scanning reports, alerts, and infection reports is a must to assist with system protection. If a network attack is discovered, monitoring that attack is vital by viewing the Internet shield status of the network. Also, you should review the certifications of each product and learn what the particular certifications denote or what test sets were used in the certification process.

At the end of the day, many AETs are able to penetrate a network without leaving a trace. Stonesoft offers the Evader testing lab for free to use in your own environment to test for AET vulnerability.

9. Consider using commercial sources to test your environment

Commercial testing is available from many vendors to detect network vulnerabilities and provide a deeper understanding of where a network may need additional fortification against threats in general and AETs in particular. Some commercial testing services are available at no cost to users. Many also provide the opportunity to launch controlled AET-borne test attacks using a variety of combinations.

10. Consider an evasion prevention system

Rather than pulling out a $1 million investment in firewalls and IPS devices, some companies are looking to Stonesoft for its new evasion prevention system (EPS). The device adds AET protection to existing networks without requiring that equipment to be replaced, all at a reasonable cost.

Chapter 10

Ten Tips for Implementing Security Vendor Management

Whether your security management comes from a new vendor or a trusted partner, you need a clear understanding of what is being done to offer you protection against the next generation of security threats. You should also know where your security weaknesses lie and what areas of your network are most at risk. The following ten tips can help ensure your security vendor management provides the safeguards your company needs and the strength where you need it most:

1. Make sure your vendor keeps it simple

Simplicity is one of the keys when it comes to network management solutions; you want your vendor to keep everything as straightforward as possible. A prime way to keep things simple is with unification and central management. Such unification should eradicate your need to use different management tools for each security product. It should also never force you to sacrifice manageability with a pseudo “unified” system that amalgamates systems that were not initially designed to be managed together. Either scenario typically results in inefficiency, high training costs, and an overall decline in security.

A truly unified system does just the opposite, providing efficient administration of your physical and virtual security elements, low training costs due to consistency, and an increase in security thanks to the ability to monitor and manage all security components in one place. Such simplicity should also come with a comprehensive view of network security, comprehensive logging with easy-to-use filtering, automatic reporting and customization options, and multiple alert methods.

2. Pursue protection against advanced threats

As technology advances, so does a new breed of threats, and you need a vendor prepared to deal with them. Advanced persistent threats, or APTs, and advanced evasion techniques, or AETs, are issues your vendor better be able to address. If your vendor is not even sure what these threats are, or tends to downplay their urgency, then a different vendor may better suit your needs.

APTs come from unauthorized users that aim to persistently target a network to gain entry and remain undetected for an extended period of time. AETs combine several known evasion methods to create a new technique that is delivered over several layers of the network simultaneously, bypassing detection entirely. You don’t want either fouling up your system.

Deep packet inspection is one security method an effective vendor may use to address APTs and AETs. Data stream-based normalization, inspection across all protocols and network layers, and flexible infra-structure patches are others. The solution should also have been tested against a wide range of threats to prove top effectiveness against the millions of combinations out there.

3. Seek software-based solutions

The most effective security management will employ software-based solutions. Software-based components allow for remote maintenance and upgrades, thereby avoiding costly on-site visits. They also allow for auto-upgrades and updates to reduce workload. The cost is also greatly reduced, eliminating the need to purchase a variety of updated versions of hardware components. Software-based solutions may be available as a physical appliance, a virtual appliance, or actual soft-ware, all with the extreme ease and other benefits derived from such a solution.

4. Demand scalability

A security vendor that offers you protection that is valid for your business today may not always be able to provide protection for your business tomorrow. Find one that can. You need a security vendor that has flexibility and ability to grow as you do, with scalable options to suit your needs without the need to invest in a whole new security environment.

Scalability should first and foremost address a change or growth in traffic patterns, as well as any changing network complexity or diversity. Effective security solutions that address a growing network include instant mass deployment and management of hundreds of devices as easily as a single device. Solutions also should avoid “forklift up-grades” that involve ripping out and replacing your entire security infrastructure. Instead, they should have the ability to phase in changes and upgrades to your existing solution as easily and smoothly as possible.

5. Investigate future costs

Even if your security vendor is on the cutting edge of bringing new functionality and capabilities to the market, it won’t mean anything unless you are privy to them. Find out if your vendor offers such advancements free of charge or if you have to pay an additional fee to enjoy the latest technology your provider offers. Obviously you want to lean toward a vendor that includes advancements without additional charges. The issue may be addressed in your end-user agreement, or you can always specifically ask about it before you invest any further.

6. Check out context-aware security capabilities

Security solutions that pay attention to context can provide some of the most effective solutions. Your vendor should have such capabilities with the best solutions involving dynamic context detection to provide for the most efficient and effective security decisions. Decisions may be made based on the time of day, location, or even the file type, with options that include GIF, JPEG, OLE, PNG, PDF, text files, and other binary files. Valuable contextual information can typically be found throughout the IT stack, and your vendor’s security management system should be able to find it.

7. Find out what happens in a buyout

With buyouts increasingly common in the ongoing sluggish economy, it’s vital to know where your

business would end up if your security company is acquired by another IT vendor. You need to be assured you will receive the same level of service and product focus that led you to choose the initial vendor in the first place. If the security vendor cannot assure you of that, you may need to look in another direction.

End-user agreements should include a clause that addresses the topic, so read it carefully before you sign. Ask specific questions and demand specific answers if the information you seek does not appear in the agreement. Make sure those specific answers are in writing to better protect you. You should also inquire whether you may break any existing contracts if an acquisition does occur and you're not happy with the results.

8. Ask for ratings and references

Make sure you ask about the vendor's customer satisfaction rating and references in your particular industry. If the vendor does not know its own rating, it may be a red flag that you're dealing with a company that does not put customer service at the forefront. After all, how would a company know what to improve if it had no idea what areas customers felt were lacking?

The most satisfied customers may come from a vendor that offers a full portfolio of on-site and call center support services and product certification training. A quality company will keep a keen eye on its performance by conducting its own customer satisfaction surveys at regular intervals. You should ask for a copy of the survey results and should also review data on consumer watchdog sites as well as through organizations such as the Better Business Bureau.

If a vendor does have complaints in its history, review how they were handled. References in your industry should reflect success with businesses that match not only your product or services but also your company's size. Don't be shy about following up and actually contacting the companies on the reference list rather than simply taking the vendor's word that the firm is pleased with its services.

9. Keep an eye on your cloud

Cloud computing is a cost-effective, efficient option for many businesses, and you want a security management vendor that knows how to handle your particular cloud strategy. Rather than adjusting your cloud to suit the security management rules, the rules should be adaptable to suit your existing strategy. Secure cloud access is at the forefront of an effective solution, and this can be had through multi-factor and multi-method authentication.

Your cloud security solution should also include a low TCO, ease of configuration, and integration into the centralized, unified management center. Enhanced reporting, minimal administration, and easy-to-use authentication methods for end users are other features to look for. Part of what makes authentication methods easy to use is having more than one authentication option. These may include a username and password pair, mobile ID synchronized or challenge options, or mobile text that sends a one-time password.

10. Find out what happens in a breach

Your vendor’s main aim is to prevent a security breach, but even with the most stalwart security measures, a breach may still occur. Find out how your vendor ensures the impact is minimized as well as how it halts the invasion from spreading throughout your entire partner, supplier, and customer ecosystem. Your vendor should have a strategy in place, as well as adequate forensics tools to investigate the breach and an acute awareness of compliance requirements.

Also consider how and when your vendor alerts you and related parties as well as how it cleans up the resulting mess. Not all breaches are handled in the same manner, and you need to be assured your vendor offers a solution that works best for you.

Conclusion

CISOs: Ask Yourself These Questions or Find Another Job

Today's CISOs have two main jobs – to secure information and to secure innovation. Sometimes they are one in the same, but they are always equally important – especially right now. Today, industries like retail, banking, manufacturing and technology are experiencing an innovation boom. And, nearly every one of these new developments are driven by the access, sharing and analysis of sensitive information across network infrastructure.

To that end, CISOs and the strategies and policies they enforce are critical not just to the security of a business – but to the furthering and implementation of the innovations that will propel the organization forward. That means CISOs should work in tandem with every strategic initiative to understand early on how it will impact information and network security, and how to mitigate risks.

Here are a few questions every CISO should ask themselves as they work side-by-side with business innovation:

1. Does your security policy match the business needs?

While the policy must address the crucial security needs, at the same time it must not be too strict to actually prevent work to be done!

2. Are you communicating clearly both upwards and downwards your willingness to be a business enabler?

Build a feedback mechanism to listen to concerns where security is causing unnecessary business harm.

3. Are you auditing and grading security functions for each department and business unit?

This helps you to identify the needed areas of improvement and to monitor the progress. Build a similar audit and grading for security cost – the inconvenience the security functions cause to the employees.

4. Do you contribute to management-level business discussions even when your input about security is not needed?

Build your reputation as a skilled, business problem solver.

5. Are you staying on top of technology and security?

Attend industry events, both large and small, and see what is trending and what might affect your role as the CISO.

From roadblock to enabler, the role of CISO is evolving. By becoming an active part of an organization's innovation strategy, rather than an afterthought, CISOs can help lead the charge in business enablement.

Joona Airamo

CISO, Stonesoft