White Paper

Allied Telesis

10 Reasons To Consolidate Threat Management

Introduction

For many years, the security in most business networks consisted of:

- a firewall at the network's point of connection to the Internet
- antivirus software, and maybe local firewalls, on workstations

However as the range of attacks has broadened and more points of vulnerability have been identified, the collection of security devices and software has grown.

A network today may contain all of the following security measures:

- a firewall
- web-traffic filtering software
- email filtering software
- an intrusion detection device or software
- Data-Leakage Prevention systems
- Distributed Denial of Service (DDoS) prevention systems
- one or more pieces of application-specific security software or proxies
- an SSL gateway
- VPN routers
- antivirus software

All of these items do a certain job very well, and each makes a significant contribution to the security of the network. However, there are downsides to a network security system consisting of multiple independent pieces.

This white paper considers these downsides, and then looks at an alternative solution for network security that avoids these problems.

Downsides of a non-unified approach

1. Each security product needs its own maintenance software and signature database updates
Security systems do not stand still. Quite the opposite–they must run fast to keep pace with the ingenious criminals who are forever finding yet more ways to attack networks.

Filtering systems require frequent updates to the databases of patterns they use for detecting malicious traffic. Additionally, to provide new capabilities, they need periodic software updates.

Any system is only as strong as its weakest link. So, a best-effort approach to maintenance of the various components is not good enough. It is important to ensure that all the separate components of the security system are up to date, all the time. This requires a disciplined approach that involves both regular review of update status of all the systems, and quick remediation of any update failures–a very time-consuming job.

2. Each security product presents its own different paradigm for management and configuration
Separate systems sourced from separate vendors will each have their own unique user interface, their own distinct ways of classifying configuration tasks, and their own ways of presenting monitoring information.

Different systems have different sets of menus to navigate and use different terminology. Each system takes time to become familiar with, and provides its own frustrations.

3. Each security product has its own quirks or limitations that need to be dealt with
Every device or piece of software has flaws, or fails to work in exactly the way one would expect. Over time, the flaws, unexpected behaviors, or limitations of the various components become evident, and decisions need to be made about how to deal with each of these. It might be a matter of working with the vendor to get issues resolved, or replacing a product that proves inadequate, or finding a configuration option that works around the issue. In each case, the experience will be different–each vendor gives a different customer experience, and each product's troubleshooting methods will vary.

4. Each security product requires periodic subscription payments
Most security systems require a subscription to be paid in order for the system to keep working. Accounting processes must keep on top of all these different subscriptions, and ensure they are all paid on time, according to their own payment cycles, to keep the security system running.

5. More products = more potential interoperability issues
As data is passed through each security product to the next, it is filtered. Headers might be updated, packets might be re-ordered, fragments recombined, and so on. The alteration that one product makes to the data may affect the operation of the next product in the chain—particularly products that are looking for traffic behavior patterns. This could lead to missed attacks, false positives being reported, or even corruption of valid data.

As each product is operating in isolation, and has no knowledge of the requirements of the other components in the security solution, it does not necessarily consider what effects its operation has on the operation of those other components.

6. More products = more points of failure

A security solution is only as strong as its weakest link. If one product in the solution fails, then the protection afforded by the solution is significantly weakened. With a multi-component solution, it is both costly and technically challenging to provide a hot-standby backup for each component. Businesses face the choice of investing the time and money into establishing and maintaining a fully redundant system, or alternatively taking the risk of downtime when a component fails.

7. More products = more power consumption

Physical devices and software applications both consume power. Power consumption in server rooms also typically has a 'double hit'–the power consumption of the device or application itself, and the power consumption of the air conditioning system required to counter-act the resultant heat generation. The greater the number of products required, the greater the power bill.

8. More passes = more latency

Each process that runs data checks takes a certain amount of time to perform each check. If checks are performed in a serial manner, then each check adds to the latency of the data transfer. For non-interactive processes like email, that is not important. But for real-time applications like VoIP, latency is a real problem.

9. A silo system misses sophisticated attacks

The biggest security threats today are those referred to as Advanced Persistent Threats (APTs). These are not isolated, opportunistic attempts to break into a network, or throw Denial of Service (DoS) attacks at it. Rather, they are patient, crafted, multi-step procedures for inserting malicious agents into a network, and then using those agents to perform damaging activities within the network.

A skilled operator will design each step of their attack to minimize its detectability. Each piece of communication involved in injecting the malicious agent, controlling it, and receiving information from it, is carefully hidden within seemingly innocent data streams.

The detection of APTs requires correlation of several factors—such as unusual DNS activity, increased Dynamic DNS requests, traffic to sites of unknown reputation, unusual amounts of data being sent out to unexpected destinations at unexpected times, and more. In an environment where security tasks are distributed across multiple products, it is not possible to recognize related changes occurring in different aspects of network activity.

10. Plugging the gaps becomes an ever-growing challenge

Building a system from a collection of specialist tools is feasible if the goal of the system is well understood, and relatively unchanging.

However, the business of cyber security is both very difficult to fully understand and forever changing.

Building a cyber defence system by selecting a set of tools and then integrating them brings with it the challenge of keeping fully abreast of new threats, and determining exactly which tools to update, replace or add to the system to keep ahead of the threats.

As attacks grow in sophistication, the task of keeping ahead of them grows ever more challenging and time consuming. Moreover, the consequences of failure to combat attacks become ever more costly.

The solution: a Unified Threat Management (UTM) Firewall

The solution to the problem of proliferating specialist-purpose security products is to replace them all with a single device—one that is designed from the ground up to provide security in the modern networking environment. Such a device, commonly referred to as the UTM Firewall, holistically combines the full range of security tasks:

- multilayer filtering—filtering based on attributes at multiple layers of the 7-layer OSI model
- virus and spyware scanning
- spam filtering
- web content filtering
- intrusion detection and protection
- SSL encryption/decryption
- IPSec and SSL VPN access concentration
- Data Leakage Protection
- IP reputation checking
- Application Control

Furthermore, UTM Firewalls perform security scanning in a “single-pass” manner. These devices employ sophisticated hardware-accelerated content filtering that can perform all the different checks in a single pass, at high data rates.

Concentrating all the security operations onto a single device means there is only one device to apply updates to, only one vendor to go to for support, only one subscription to pay, only one user interface to become familiar with, only one device’s worth of power to provide, and so on.

Significantly, as new types of threat emerge, UTM Firewall vendors will provide exactly the right enhancements to their integrated solution to keep ahead of threats. The task of plugging the gaps then lies with the vendor, who has the specialist expertise in network security.

A fully integrated solution can also detect the changes in different aspects of network activity that are the only indications of the presence of a highly sophisticated attack.

On top of all this, packing the security solution into one device makes high availability much more feasible. A resilient pair of UTM Firewalls is easy to provision, whereas provisioning redundant pairs all the way along a chain in a multi-component solution is extremely difficult.

Conclusion

Having a network security system that consists of multiple independent products, which each do a different and specialized job, brings with it a long list of downsides. Each security product must be maintained, updated, paid for and powered. Each product presents its own limitations, and its own issues with configuration, management and interoperability. More products mean more points of failure, more latency, and more difficulty identifying attacks and plugging holes.

Consolidating threat management is the solution to these problems. Having all of a network's security needs unified within a UTM Firewall means that network is not only safer, but also cheaper to purchase, run, and manage—both now and into the future.

About Allied Telesis

For over 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Autonomous Management Framework™ (AMF) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and "things"—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis**.com

C613-08030-00 RevB