Building Trusted Networks:
Gaining Control of IT Security

VERSION 3
JANUARY 12, 2006

By
Nicholas John Lippis III
President, Lippis Consulting
Table of Contents

- Introduction
- 1.0 The Dangerous Status Quo of IT Security
- 2.0 Trusted Network Architecture Model
- 3.0 Secure Domains Wrapped Around Business Process
- 4.0 Implementing a Network-Based Enterprise Threat Defense
- 5.0 Summary
- About Nick Lippis
- About Lippis Consulting
Introduction

The existing appliance-based strategy of enterprise threat defense is not capable of defending an enterprise against an increasingly harmful and rising number of exploits while allowing IT staff to gain control of IT security. A network-based enterprise threat defense strategy offers the best approach to gaining control of the IT security problem and moving IT security staff into a more proactive role.

This paper explores the attributes and benefits of a network-based enterprise threat defense strategy.

1.0 The Dangerous Status Quo of IT Security

Defenses available to IT departments to protect against a litany of daily threats to their enterprise networks are wide and broad. Unfortunately there is little to no automated coordination between defensive IT security technologies such as firewalls, intrusion detection/protection systems (IDS/IPS), network-based anomaly detection (NBAD) devices, patch management systems, VPN appliances, etc. This fragmented approach to IT security along with an exponential increase in the number of threats/exploits has given rise to the status quo of helter-skelter attack mitigation.

The status quo of attack mitigation is unfortunately a less than organized and structured process. An exploit enters the enterprise. It propagates quickly, infecting a large number of servers, desktops, laptops and eventually, mobile end-points. Large IT firms issue warnings, identify the exploit signature and send out hot fixes or patches to the industry. IT departments spend the next several days cleansing systems in an attempt to bring the corporate network back to normal operating performance. During this process knowledge workers and IT staff are distracted until the exploit is contained, patched and the systems cleansed. Depending on the severity of the exploit, IT staff can be totally consumed with patch management and system cleansing, interrupting knowledge workers by taking over their computing systems in the process. This is a lengthy and reactive process with little to no warning and often accompanied by disorder. In short the status quo does not scale and it’s woefully inadequate to fix the IT security problem which is only getting larger with more severe consequences.

The stakes are getting higher. IT security vulnerability and exposure has long surpassed the point of being a nuisance. Hackers are no longer rogue individuals seeking a thrill; they are professional, organized IT criminals seeking to steal information and create real damage. Organizations such as the 4000 member shadowcrew.com, which set up an international clearing house site, much like eBay, for stolen credit cards and identity documents, are professionals targeting and stealing from corporations and individuals. It’s reported that shadowcrew.com made some $8 million in two years. Then there’s HangUp, a Russian organized IT crime group who distributed the Scob worm on various legitimate online stores which would steal passwords and other identity information after a user visited the online store and entered their personal information and send them back to HangUp. According to the International Crime Complaint Center the number of net fraud complaints has skyrocketed from a little over 6,000 in 2000 to over 200,000 in 2004.

As if it wasn’t bad enough having to defend against exploits and their ability to wreak havoc on business process, the US Federal Government and European Union have put in place new legislation and presidential initiatives which place evolving constraints on data privacy, access, archiving and integrity, and force firms to publicly disclose security breaches. Some of these are the Homeland Security initiatives, the popular Sarbanes-Oxley Act, Gramm-Leach Bliley Act, Presidential
Decision Directive 63 (PDD 63), in the health care industry the Health Insurance Portability and Accountability Act (HIPAA), and in Europe the Basel II Accord, which requires accounting for IT security vulnerabilities on the balance sheets of European companies. Non-compliance with any of these directives and acts carries severe repercussions for employees, executives and enterprises at large.

At the same time, as incidents skyrocket, IT budgets, technology, skills and the ability to react are linear with a near zero slope, placing a corporation far behind the propagation velocity and frequency of exploits. The vulnerability gap grows larger with every new exploit. The days between an exploit and an associated patch, to delete or neutralize it, is shrinking precipitously. For example, there were 331 days between the Nimda exploit and its patch while the difference between the Blaster exploit and its patch was only 25 days. The recent Zotob patch was released by Microsoft in under 7 days after it was identified. With an exponential number of exploits and patches being distributed in shorter and shorter times, IT security personnel can be consumed with the reactive hot fix and patch management cycle.
The status quo will not work to stop today’s sophisticated hackers, malicious employees and organized cyber criminals. Part of the problem is that the speed and volume of exploits have also outpaced the ability of the vendor community to deliver solutions. IT security companies have been packaging and delivering point security solutions to the industry in the form of appliances. While appliances have their place, they also create an acquisition cost barrier of entry and drive up security management operational cost. For example, it’s impractical to deploy four devices in every remote office to deliver firewall, IDS/IPS, VPN, and NBAD services, but that is exactly what some firms are faced with. The cost is just too high. Also, the difficulty of managing four different security devices with four different management interfaces does not contribute to reducing IT security operational spend. This appliance-based enterprise threat management strategy is systemic throughout the enterprise, be it in the data center or now within corporate offices, as the requirements to increase segmentation and firewalling of different groups has expanded.

The appliance-based strategy of enterprise threat defense is not capable of defending an enterprise against an increasingly harmful and rising number of exploits while allowing IT staff to gain control of IT security. In short, a pervasive appliance approach to threat defense is too expensive in both acquisition and operational cost. An IT security staff will not be able to gain control of exploits with the status-quo of a perimeter defense or hard shell and lack of internal defenses or soft core. There is no single perimeter to defend.
A network-based enterprise threat defense strategy offers the best approach to gaining control of the IT security problem and moving IT security staff into a more proactive role. An all-encompassing threat defense approach to IT security is needed which incorporates appliances and is network-based. The network-based enterprise threat defense strategy is highly integrated into and embeds security features deep within the network fabric of Ethernet layer 2 and layer 3 switches, WLAN devices and routers. This strategy allows IT staff to “network” security appliances so they may share valuable threat information and when required, consolidate appliances.

The benefits and promises of a network-based enterprise threat defense strategy includes lower operational and acquisition cost to defend enterprise IT assets. With an increased number of exploits contained and neutralized a shift from reactive to proactive IT security management can take place. By deeply embedding security features and functions into the network fabric, a network can be adaptive and responsive to threats and automate exploit mitigation. The real value of a network-based enterprise threat defense strategy is the reduction of successful attacks that cost corporate credibility, revenue, productivity and profits.

2.0 The Trusted Network Architectural Model

The network-based enterprise threat defense architecture is a trusted network based upon three major components.
Three Architectural Components of Network-Based Enterprise Threat Defense

**Component 1: Client or Host Software**
The first architectural component of enterprise threat defense is client or host software. Anti-X client software is the first and zero day responder to exploits. Their job is to contain an exploit before it propagates through an enterprise network infecting other systems. Client software also keeps a status of the end-point's posture, i.e., operating system, anti-virus version, file register, memory, file execution read and write, dynamic execution space, etc. This posture is assessed by network access control, discussed below.

In addition to Anti-X software the TPM or Trusted Platform Module hardware/chip developed by the Trusted Computing Group (TCG) provides a root of trust for every end-point. That is, every end-point will have as its basis certain information that can be trusted without the prospect of corruption. The TPM ensures the trustworthiness of integrity measurements and works with Anti-X client software, providing trusted system posture information that is communicated to switches during network access control sessions.

There are three major categories of clients or classes of users. Users can be employees, contractors or guests. Users gain access to the enterprise network over a wide range of access vehicles such as LANs, WLANs, IPSec, SSL, mobile wireless networks, etc., which are independent of geographic distance. The amount of control IT departments have over end-points varies. Control is highest with employees and contractors while IT departments have the least control over guest end-points.
Component 2: Network Access and Containment Control
The second architectural component is the security services embedded within the network. Controlling access to the network and containing exploits if and when they break through defenses is the job of embedded network security services. To gain access to IT resources all end-points will be assessed based upon their posture. If their posture does not conform to a set of policies defined by the IT department, they are quarantined into a safe VLAN until they are in compliance. The network may offer a pop-up menu instructing the user on how to bring their system into compliance.

Network access offers IT departments an important tool to control who and what has access to all networked IT resources. Gone are the days when every employee plugged into the network and was offered universal access to all IT assets. Network access control not only controls access to the network but access to all networked resources. During access control, users can be assigned quality of service and placed into a stratified set of network services. For guest users, where IT departments do not have control over client software, controlling network access offers a check point to assess the guest posture, scan for exploits and apply policy, thus limiting network resources available accordingly.

In addition to controlling network access, controlling the propagation of exploits or their containment is the second most important embedded network security service. The network collects a security posture of the network and is alarmed based upon anomalous behavior. Once alarmed, the network has the ability to contain the exploit by shutting down ports, flows, VLANs, etc.

Network containment is analogous to law enforcement putting road blocks across a diameter of area to contain a suspect before they escape and do more harm. Another example is the federal US government discussing containment of cities or towns in the case of a pandemic brought on by an Avian Influenza flu virus. Containment of exploits is no different. The automated and adaptive function of network containment is complex as it’s based upon a sophisticated back-end control.

Component 3: The Back-end
To explain the back-end, a law enforcement analogy is helpful. Assume a vehicle is pulled over by the police. Police enforcement use the license plate number, registration and driver’s license to assess the privileges associated with the driver. In short the certificates are checked for their authenticity and driving records associated with them. All this information is referenced against a data base which enforcement uses to assess the level of threat the driver poses. An outdated driver’s license could result in the loss of driving privilege. An old inspection sticker will result in a fine and possibly the revocation of rights until the vehicle is in compliance. Too many speeding tickets and the driving privileges may be suspended or revoked. The tool which the officer uses in his/her assessment of the situation and subsequent actions is a large nation-wide data base.

The enterprise network will leverage a back-end set of data bases to do the same. This is the third component of enterprise threat defense. During network access control, the network checks a client’s posture and interrogates a set of data bases and policy resources to assess the client’s identity and privileges. AAA or Authentication, Authorization, and Accounting once used for dial-in remote access is taking on a new and larger role in enterprise security. A back-end of data stores linking unified directory services, employee profiles, device profiles, AAA databases, etc., are consulted to segment users into classes and enforce access privileges. For
example, the ProCurve Networking by HP’s Identity Driven Management software does just that.

In addition to network access policy enforcement, the back-end also is empowered with network configuration resources. For network containment, the back-end will have multi-vendor network configuration control and a centralized view of the network’s posture. The triggers that invoke network configuration changes such as shutting down subnets, VLANs, ports, flows, etc., are an area that is evolving. The trigger will be based upon the analysis of real time anomaly behavior detection and signature data.

For example, the ProCurve Networking by HP’s Virus Throttle technology acts in this way, detecting anomalous behavior and taking action on Ethernet switch ports accordingly. Virus Throttling monitors network behavior across Ethernet ports to detect virus propagation. If anomalous virus traffic behavior is detected on a ProCurve 5300xl port, it will slow down traffic on that port and notify ProCurve Manager Plus so further action can be taken if warranted. Network-based anomaly detection functionality is fully integrated into the switching fabric rather than housed in a separate appliance.

<table>
<thead>
<tr>
<th>Type of Defense</th>
<th>Host Based</th>
<th>Network-Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Anti-X, personal firewalls</td>
<td>IDS/IPS, FW logs</td>
</tr>
<tr>
<td>Behavioral</td>
<td>Next generation anti-X software, Cisco Trust Agent.</td>
<td>Virus Throttling, some IDS/IPS products, Cisco Guard and Cisco Traffic Anomaly Detector, NBAD or Network-Based Anomaly Detection (Mazu, Arbor, Lancope)</td>
</tr>
</tbody>
</table>

Over time the technology of exploit containment will rely increasingly upon collaboration between network security devices and elements that share state or posture information between systems to make better mitigation decisions. For example, dampers which act like shock absorbers to networks being flooded by bad packets will slow down or rate limit traffic by extracting the bad packets out of flows. There are trust models also being explored based upon peer systems (desktops, laptops, servers, etc.) that act like tattle-tales informing the back-end when one system starts behaving badly. Based upon tattle-taling, the back-end may distribute sentinels that mitigate day-zero exploits or take a system off the network until its exploits are mitigated.

Back-ends will have live feeds into public security services which issue warnings, the latest exploit signatures and behavior profiles so that networks can react accordingly if these exploits are identified within their network. Clearly the industry and IT security staff will cautiously turn on the auto-pilot step by step until it’s trusted.

The context of an alarm or behavior will play a large part in determining the network’s mitigation response. Just like responses to emergency calls are weighed by the context in which they are received, so will network mitigation responses. If a call into the emergency 911 service is made by a reasonably calm person who describes an accident, the 911 agent will issue an ambulance to the scene of the accident. If another call into 911 is made by a hysterical person and gun shots are
heard in the background followed by more screaming, the response may be a swat team, police and an ambulance. Context in the alarm will measure the mitigation response.

### 3.0 Secure Domains Wrapped Around Business Process

With the tools of network access control and containment features deeply embedded within the network fabric collaborating with the Trusted Network back-end, IT departments can now guard business process by wrapping them within "Secure Domains".

To understand secure domains, it is helpful to think of virtual LANs or VLANs. VLANs describe a technique to create, modify and in essence manage broadcast domains within LANs. VLANs allow network designers to increase performance by reducing the number of end-systems per broadcast domain, provide logical barriers between groups and applications and place different applications in higher priority VLANs.

There is a huge requirement to segment networks into security domains, which is strikingly similar to the need for broadcast domain segmentation in the ’90s. Today many corporations are installing internal firewalls in front of sensitive resources inside the enterprise network. This is a crude, first generation secure domain. The requirements for secure domains are as vast as the number of companies in the global economy. Some firms require separating departments, some need to group select desktops, servers and applications, some want to create extranets with suppliers, partners and customers. Some firms and universities provide services for the federal government, which places strict restrictions, and consequences, on access to data, systems and information requiring a secure domain to be wrapped around this business process. Then there are the legislative and presidential initiatives mentioned above, which mandate that corporate boards in essence place secure domains around certain privacy information plus financial work product and business process. The simplest definition of a secure domain is the grouping of IT resources into a protected networked space. This protected space will be as porous or impervious as the corporation requires.

Can you build a secure domain today? The answer is yes, but it’s very expensive in both acquisition and operational cost. Just like with Ethernet LANs, before VLANs network designers could install routers between broadcast domains but this design was cost prohibitive. So too are secure domains implemented with today’s technology. Today network designers would have to install firewalls around IT resources to approximate the service as a secure domain. And if you want to know if there is an intrusion into that space the designer can install an intrusion detection system or IDS. And if you don’t want to be exhausted with reams of alarms and alerts the network designer can install an intrusion protection system or IPS. And if you want to provide zero-day attack prevention or mitigation in that space, the network designer can install a Network-Based Anomaly Detection or NBAD device.

To deliver on the promise of secure domains, firewall, IDS, IPS, NBAD, virus and worm scanning security features need to be deeply embedded in the network fabric as mentioned above and their configuration and management centralized and virtualized. The management interface and configuration for secure domains is key to their adoption. It is within secure domains that a stratified segmentation of a user population can be designed. If different classes of users obtain different access methods and quality of service, the network needs to provide the mechanism to implement this stratification.
Part of this stratification is the segmenting of services on a per-user level. Since VLANs are a layer 2 construct they lack the granularity to parse services per user. Secure domains are a layer 3 construct which will increase granularity to allow segmentation on a wide range of objects such as ports, users, data, IP addresses, applications and IT resources such as printers, e-mail, servers, scanners, fax, etc. In short, secure domains that control network resources on a per-service level, per-user basis promises to be the most effective method of securing and guarding business process. With network controls implemented on a per-user basis, secure domains offer a solution to the extracting or transferring of sensitive corporate information out of the enterprise from within.

The ProCurve Networking by HP’s Identity Driven Manager (IDM) software provides this functionality by dynamically managing network devices to automatically apply security, access and performance settings to network infrastructure devices based on user, device, device posture, location and time. IDM automates the configuration of intelligent edge devices to provide unique behavior/segmentation for every individual or group. It ensures switch and access point features make the correct decisions and enforce policies at network access. This creates the ability to manage and facilitate:

- Network Access Control
- Access Rights – Based not only on the individuals and their group associations, but also on the device they are using (i.e., PC, laptop, PDA, or VoIP phone), day, time and location and its compliance to network policy
- Policy Enforcement – On a per-user, per-session basis

4.0 Implementing a Network-Based Enterprise Threat Defense

As with any enterprise-wide project, implementing a network-based enterprise threat defense requires planning, preparation, design, implementation, operation and optimization. A security audit, posture assessment and penetration testing usually encompass the planning and preparation phase. Next, business requirements, regulatory compliance issues and technology readiness drive the design which is followed by implementation and operation. Staging is very important in the design and implementation phases.

**Stage one is the implementation of existing appliance-based defenses.** New security services will more than likely be delivered first in an appliance form factor. The industry is currently in the vertical integration stage where many security functions such as firewall, IDS/IPS, VPNs, etc., are being integrated into one device. As anomaly behavior detection technology is more widely implemented, the vertical integration of threat defense will shift to a more horizontal network-based implementation.

**Stage two is implementing anomaly behavior-based client software** on end-points. As the appliance market progresses IT departments can add strong defense to their end-points by implementing not only anti-virus software but more importantly anomaly behavior-based client software.

**Stage three is the deployment of network access control** to existing network infrastructure. Network access control when combined with appliances and anomaly behavior-based client software will dampen out or bolster exploit propagation defenses.
**Stage four is building the back-end.** Building the back-end of enterprise threat defense architecture will add value to access control by injecting policy into the access process, thus providing the IT department with a large number of options with which to control IT resources. Available options will include adding quality of service, restricting access to resources, restricting file transfers or copying of files on personal storage devices, etc.

**Stage five is implementing network containment services.** The back-end will evolve to include exploit containment and automated mitigation services. While automated mitigation may leave network executives a bit uneasy right now, IT departments will gain confidence and trust slowly before they turn on the auto-pilot. This trust will be gained over time. It may take a few business cycles before IT executives become comfortable with high levels of adaptive and automated mitigation which involve shutting down ports, segments, VLANs, flows, etc., within the network to contain outbreaks. The illustration below shows a five-stage process toward network-based enterprise threat defense implementation.

Many organizations will implement network security at different stages or they will implement multiple stages in parallel. Vulnerabilities and risk level usually dictate the staging of threat defense implementations. The five stages identified above parallel the major industry initiatives which are underway. Stages 1 through 3 represent available technology with Stage 3 being in an early phase. Stages 4 and 5 are early as well with Stage 5 being the furthest from product or service implementation.
While broadly based containment-based adaptive threat defense mechanisms may be a 2006/2007 event, vertical consolidation of security features is well underway. In fact even today’s virus throttling and vertical adaptive threat defense appliances when combined with back-end systems, such as IDM discussed above, client-based behavioral defenses and access control will go a long way toward allowing network security administration shift from a reactive to a proactive posture, giving staff proper time to schedule patches, contain outbreaks and get out of the security crisis mode of operation. In short, this will allow IT personnel to gain of control security administration.

5.0 Summary

As the number of sophisticated and harmful exploits increases exponentially so too does the number of hot fixes and patches. This cycle of exploit propagation and patch management is expensive to administer and increasingly ineffective. IT departments need to shift toward offense rather than defense to secure their IT assets and gain control of their resources. A new field is emerging called information security which provides situation analysis and vulnerability assessment for large systems. How do you assess the risk of 100,000 devices? There is a massive amount of data that a network provides concerning behavior. The IT industry and academic institutions are focusing on methodologies to collect, sift through and take action on anomalous behavior. In the same way the human body lives with some illnesses and viruses so too can networks. In a network of 100,000 end-points, are ten infected end-points out of 100,000 an acceptable level of risk? What level of illness is acceptable? How much risk your network can accommodate at a reasonable reaction rate is the new way to manage risk.

One thing is for sure, exploit mitigation and enterprise threat defense is network-based rather than end-point or server-based. The network is the platform to administer and launch threat defenses. In this paper I discussed the architectural components of a network-based enterprise threat defense strategy which will return control to IT departments by allowing them to be more proactive in their reaction and management of threats and risk. This strategy is built upon leveraging existing security appliances, technology and network infrastructure. The promise of this strategy is to deliver to IT departments a network which is adaptive to existing and new threats and is capable of automatically mitigating exploits in real time.
About Nick Lippis

Nicholas J. Lippis III is a world-renowned authority on advanced IP networks, communications and their benefits to business objectives. He is currently working with clients developing converged network architecture, which includes IP telephony, secure networks, wireless LANs, internet data centers and storage area networking. He is the chairman and host of the Trusted Networks 2005 Symposium, a conference where corporate network architects and designers learn and share industry best practices. Mr. Lippis hosted thirty-seven sponsors and four hundred and sixty delegates during his Enterprise Networks 2004 conference in Boston.

He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cigitel, Cisco Systems, Nortel Networks, Lucent Technologies, 3Com, Avaya, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee and many others. He works exclusively with CIOs and their direct reports. Mr. Lippis possesses a unique perspective of market forces and trends occurring within the computer networking industry derived from his experience with both supply and demand side clients.

Mr. Lippis founded Strategic Networks Consulting, Inc., a well-respected and influential computer networking industry-consulting concern, which was purchased by Softbank/Ziff-Davis in 1996. Mr. Lippis was named one of the top 40 most powerful and influential people in the networking industry by Network World. For nine years Mr. Lippis reached over 120,000 purchasers of networking equipment and services through his monthly column “Lippis on Internetworking” published in Data Communications magazine. He was a contributing editor and columnist for Tele.Com magazine reaching over 80,000 service provider professionals monthly.

He currently writes the “Lippis on IP Communications” column for Network World reaching 180,000 in print and 850,000 online. He publishes The Lippis Report, which is distributed to over 360,000 senior IT executives around the world. Mr. Lippis’ reach exceeds 1,400,000 readers. He is a frequent keynote speaker at industry events and is widely quoted in the business and industry press.

Mr. Lippis received his Bachelor of Science in Electrical Engineering and his Master of Science in Systems Engineering from Boston University. His Masters' thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.
About Lippis Consulting

Lippis Consulting provides a wide range of enterprise consulting services to enable corporate technology executives to maximize their IT budget and existing infrastructure. Our consultants have extensive experience working with F1000 clients, enabling them to align their IT strategy with corporate business objectives.

Lippis Consulting Services include:

- IT budget spend analysis and industry comparison
- Total Cost of Ownership (TCO) analysis
- Alternative technology assessment (ROI)
- Network infrastructure and security audit
- Infrastructure optimization analysis
- Network design & architecture
- Outsourcing options
- Carrier services evaluation & rationalization
- Strategic vendor/partner selection