



# Managed Security Services

Over the last fifteen years, libraries have gone through a transition from being primarily a repository of paper based reading material to very sophisticated technology centers. In fact, part of a library's mission in today's environment is to help their patrons bridge the "digital divide". Several studies published over the past two of years indicate a growing trend in libraries as the sole provider in communities to free public computer and internet access. Unfortunately, increased access to technology in libraries comes with some inherent challenges.

Security attacks coming from both inside and outside of the library are growing in quantity and frequency, as well as becoming more impactful to a library's operations. With so many different types of security attacks targeting our libraries, it is becoming difficult to identify which threats pose the greatest risk and then in turn manage those risks accordingly. Unfortunately libraries are typically not in a position to have a "security engineer" on staff to mediate the IT security challenges facing their organizations today. This is where NLE's **Managed Security Services** come into play.

**Managed Security Services** from NLE provide the physical equipment and professional expertise to manage the security safeguards in a library's internet attached network. NLE offers complete systems monitoring and proactive responses to block, detect, alert, report, and respond to any kind of incident or threat which may occur.

NLE's **Managed Security Services** enable libraries to benefit from a reduction in operating expenses, staff/IT time spent on technical support, and the security concerns a library has by being connected to the Internet. This peace of mind is accomplished through a sophisticated combination of Fortinet FortiGate Security Appliances, our Firewall Analyzer, and the highly technical skills of our Security Operations Team.

**Managed Security Services** include the following features:

## **FIREWALL**

The firewall your library utilizes should have complete control of how information flows in and out of your network to the Internet. The firewall functions through a strict set of complex rules called security policies that are used to allow or restrict connections to or from your network to the Internet. The Fortinet devices used for this solution are appropriate for networks of all sizes and complexity, ranging from small community libraries to large consortiums.

## **INTERNET CONTENT FILTERING**

As part of the customized Internet Connection Profiles, Content Filtering offers an easily understood approach to organizing the Internet into 56 web page content categories. These categories range from Spyware to Pornography and contain the largest and most accurate content database of the Internet, covering over several billion web pages. In conjunction with 24x7 Reporting and Alerting, detailed listings of websites visited by individual users and workstations are available. This provides the ability to monitor staff internet usage and to determine possible violations of your library's security and content policies. Selected categories can be actively blocked with custom user notification screens and alerts.



# Managed Security Services

## **GATEWAY BASED ANTI-VIRUS**

As part of customized Internet Connection Profiles, the Gateway Based Anti-Virus system can scan and remove viruses and infected files before they enter or exit your network. The ICSA Certified antivirus scanner allows for complete virus scanning of all web traffic, email traffic, and file transfer (FTP) connections. The service also has the ability to block any specific file types from passing through the system. This includes files that may contain sensitive data such as database files, Word and Excel documents, or files that contain a digital signature which identifies their sensitivity.

## **GATEWAY BASED ANTI-SPYWARE/GREYWARE**

Spyware and Greyware are currently one of the most prevalent problems facing Internet Users. These attacks can range from applications that track your every move on the Internet, produce pop-ups, or dial your modem to 1-900 based "pay numbers". As part of customized Internet Connection Profiles, the Spyware system identifies these applications and actively blocks them prior to their reaching your computer. In conjunction with Internet Content Filtering, the Gateway Based Anti-Spyware system offers unprecedented protection from these types of attacks. Reporting and Alerting for this service provides detailed information and notification of Spyware and Greyware infected files that have been blocked from entry into your network.

## **GATEWAY BASED ANTI-SPAM**

As part of your Internet Connection Profiles, the Gateway Based Anti-Spam uses a variety of methods to identify spam entering your network. This service works with any type of email service. Emails are identified by content, sender address, sender location on the Internet, email header, or through databases of known addresses of spammers. Simple mail server or mail client rules allow for complete customization of how mail is processed upon identification. Detailed information regarding statistics of the anti-spam system and emails identified is available through the Reporting and Alerting System.

## **NETWORK BASED INTRUSION PREVENTION & DETECTION**

Identifying and actively blocking attacks and malicious programs in real time is the primary function of the Network Based Intrusion Protection & Detection System. This ICSA Certified service combats some of the most prevalent problems facing library networks today: Peer-to-Peer File Sharing applications, Instant Messaging, Back Door Hacking Tools, and over 1000 other Internet Attacks. When used in conjunction with the Reporting and Alerting Systems, detailed information regarding blocked attacks and alerts can be reviewed on demand.



# Managed Security Services

## **VIRTUAL PRIVATE NETWORKING**

Virtual Private Networking (VPN) provides secure communications over the Internet for employees, business partners, and clients. This service allows for secure connections to and from remote networks or for remote staff users. Your network can be configured to utilize IPSEC VPN, SSL VPN, or PPTP VPN. The Reporting and Alerting system can provide detailed connectivity reports regarding these connections.

## **INTERNET AUTHENTICATION**

Internet Authentication can verify that only permitted users are accessing the Internet via your network. The service can utilize an internal database of users, integrate with a Windows Domain Controller, or a Radius Authentication Server. After a user is authenticated their access of the Internet can be monitored based upon their user name. This service also allows for authentication of Intranet Servers, further simplifying user management of internal resources.

## **BANDWIDTH SHAPING**

With the evolution of VoIP technology (Voice Over IP) the importance of being able to manage how your bandwidth to the Internet is utilized has never been more important. The priority of the data packets that make up voice and video applications is far greater than that of simple web surfing or email. Bandwidth Shaping allows for customized QOS (Quality of Service) for your most critical internet applications and remote communications.

## **SYSTEM HEALTH & INTERNET AVAILABILITY**

NLE will immediately discover any problem with your connection to the Internet as we continuously monitor the status of your system's Health & Internet Availability. We frequently check your device to ensure memory and processor utilization are within tolerances; as well as ensuring your network is able to access the Internet. In the event of any irregularity, NLE immediately creates a trouble ticket and investigates the issue. Through the Reporting and Alerting system you can receive immediate alerts of network outages.

## **24x7 REPORTING & ALERTING**

An essential component of our service is the 24x7 Automated Reporting & Alerting System and Firewall Analyzer. This web based reporting solution is completely hosted by NLE, meaning that no additional hardware, software, or expensive server licensing is needed. The service offers over 150 dynamic drill down reports which can provide unlimited means of viewing Internet activity. Moreover, the system has a fully programmable alerting system that allows you to be notified for specific events through a customized alert profile. Scheduled reports are also available, delivering the information you need directly to your inbox at the time and date you specify.



# Managed Security Services

## **CONFIGURATION, SUPPORT, MANAGEMENT & HELPDESK**

All of the services listed above can be completely managed by NLE or in conjunction with your IT Team. Typically, initial configuration, firmware updates, unlimited policy changes, support requests, and programming updates are included in this service. The service also provides access to our knowledgeable support professionals to answer any questions you may have about this service or Internet related issues.

### **FEATURES:**

- Expert Fortinet Firewall Management
- Monitoring of firewalls from our Security Operations Center
- Alerts clients of unexpected events
- Provides firewall maintenance, conducting most firewall changes within four hours of client request
- Perform regular configuration backups
- Real-time intrusion detection reporting for immediate notification of hostile activity
- Overcome security challenges resulting from limited resources or a shortage of skilled security engineers on staff
- Defend your library's computing assets from loss and/or damage from network attacks
- Protect critical data and sensitive information from compromise or modification
- Report overall firewall activities, system configurations and change management
- Provides support for Virtual Private Networks (VPNs)

**Call for your quote today!**

**801-377-0074**

**or email**

**[sales@nle.com](mailto:sales@nle.com)**