Network Monitoring Policy for Troubleshooting

Cleveland Branch Office Network

Kevin O'Neal

DeVry University

NETW208: Accessing the WAN

Submitted to:

Professor: Hopkins

Date: 10.-21-2012

2. Network Monitoring Policy

In order to provide feasible network monitoring, baseline creation and effective troubleshooting, a network monitoring policy must be created and implemented. The following network monitoring policy is an example of what must be implemented to define the security procedures and company policies concerning network monitoring….

Cleveland Office of You Decide Company

Network Monitoring Policy

October 21, 2012

I. PURPOSE

The purpose of this document is to outline You Decide Company policy regarding the monitoring, logging and filtering of network packets that traverse the Cleveland Office Network. The goals of this policy are:

A. To maintain the integrity and security of the Cleveland Office's network infrastructure and information assets,

B. To collect information to be used in network design, engineering, troubleshooting and usage-based accounting for creation of a baseline to be used for troubleshooting and performance monitoring.

This policy acts in conjunction with any policies referenced that is required for connection to the Cleveland Office Network, as well as the use of and access to You Decide Company information resources by any division or organization within the You Decide Company.

II. INTRODUCTION

The You Decide Company considers all electronic information transported over the You Decide Company network to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as private and confidential. Any inspection of electronic files, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by You Decide Company policies.

III. SCOPE

This policy applies to all users of the You Decide Company information resources over networks that cause traffic to traverse the Cleveland Branch Office Network. The policy extends from the Network Access Point (NAP) to the end-user machine.

3. Network Monitoring Policy

IV. POLICIES

A. Monitoring network traffic at the You Decide Company will involve only the collection of packet header information, not the packet data, unless required to check for viruses, to monitor the improper release of confidential employee information, or for intruder detection.

B. Two entities at the Cleveland Branch Offices are authorized to routinely monitor traffic on the network. These are authorized personnel within the Network Department and the You Decide Company's Security Department.

C. Intranet traffic may be monitored by local department(s) and division(s) at the discretion of the Cleveland Office Branch Manager, Department Head, or the Corporate Manager. If any department or division intends to perform network monitoring for purposes other than routine network operations, diagnostics and maintenance, the network administrator will notify the Security Department of such network monitoring activity.

i. The use of sniffers or devices, which operate in promiscuous mode, are to be used only by the authorized local network administrator for diagnostic purposes of intranet traffic only.

ii. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines, and must respect users' rights to privacy.

D. Personnel authorized to analyze network flow as set forth in paragraph B above, will not disclose any information realized in the process without approval of the Cleveland Office Branch Manager or department head. Departments may request flow information with the Corporate Manager's approval. The method to request this information is as follows:

i. A memo from the Branch Office Manager or department head must be sent to the Corporate Manager requesting network flow information generated by a Cleveland Office Branch user's machine.

ii. The Corporate Manager must determine if the request merits the involvement of the Network Administrator or Security Department and authorize their involvement via the appropriate form.

iii. The Network Administrator or Security Department will analyze the flow information to establish the security risk to the You Decide Company. If there is a risk, the Network Administrator or Security Department will proceed to examine the flow of the packets, and will take the necessary action. If there is not a security risk, but other issues are identified, (e.g., acceptable use) the Network Administrator or Security Department will return the request to the Corporate Manager with their recommendations.

iv. The Network Administrator or Security Department will then release the requested data to the requesting employee or department head.

E. The Network Administrator or Security Department will be the contact for resolution of anomalies or other suspicious activity noticed by their scrutiny.

F. The Network Administration Department will monitor the network 24 hours a day, 7 days a week. All network failures and excessive utilization will be reported to the technical staff for problem resolution or design enhancement. The Network Administrator will act as the Point of Contact for network traffic problems.

4. Network Monitoring Policy

G. Employee Electronic Transmission Monitoring

This policy does not govern the monitoring of employee electronic transmissions for job performance evaluation.

H. Internet Services Monitoring

Management and employees should be aware that logs are generated by the various Internet services used on the network, including email and web access and network flows. While it is not the policy of the You Decide Company to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the You Decide Company's WAN Internet links.

I. Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed. Electronic logs that are not destroyed may be subject to production if a relevant request is received.

J. Disconnect Authorization

The Network Administrator or Security Department has the authority to discontinue service to any network or network device that is in violation of this policy or has demonstrated a hindrance to network performance. If the threat appears to be security-oriented, consensus by one authorized Network Administrator or Security Department representative will be required to discontinue service. Network Administration or Security Department representatives will inform the local network administrator and inform them of specific actions that must be taken to avoid disconnection. If the Network Administrator is not responsive, the Security Department may discontinue service. Network Administration or Security Department representatives will inform local administrators of corrective actions that must be implemented to avoid disconnection. If corrective actions are not implemented within a reasonable time period, the Security Department may discontinue service.

K. Enforcement

The Network Administrator or Security Department will cooperatively utilize information about traffic flow on the You Decide Company Network and Domain Name System (DNS) data space to enforce provisions set forth in the Network Connection Policy, the Network Monitoring Policy and the You Decide Company's Security Policy and State and Federal laws.

….**this** example is a modified policy from the University of Utah. It clearly defines the security, procedures and layers of authority that one must traverse in order to monitor any network traffic on their campus backbone network. Once these policies are clearly understood and accepted, a baseline can be created.

The process of baseline creation is a time consuming task. The documentation of network devices, network configuration table and end-system configuration table is critical. The use of networking monitoring tools like network management systems (NMS), knowledge bases, baselining tools and protocol analyzers are necessary to create a useful baseline. Other baselining procedures include:

deciding what data to monitor, identifying devices and ports to monitor, determining the duration and appropriate times to monitor traffic flows and finally measuring the performance data.

There is no industry standard approach for setting baselines. However, there is a set of best-practice guidelines that have been put together in a centralized framework. This is known as the Information Technology Infrastructure Library or ITIL. Within the ITIL framework there is a set of ITIL monitoring tools designed to take advantage of configuration databases and applications for IT service management. Other such best-practice guides include the International Foundation for Online Responsibility and InfoSec. These guides help to set a standard for network performance monitoring and internet ethics and monitoring.

Once baselines have been implemented, monitoring and using the data collected for troubleshooting is part of a preventative maintenance plan. Some hardware tools to aid in network monitoring and troubleshooting are: network analysis modules (NAM), digital multimeters, cable testers, cable analyzers and portable network analyzers. These devices will need to be calculated into the network budget. Also, hiring the qualified personnel to operate these devices and monitor the network for anomalies from the baseline should be considered. This individual or individuals should be qualified and possibly certified network IT professionals. The hiring of "certified" network IT's will help lower training time and costs. This should make for efficient network administration and maintenance.

As mentioned earlier, the documentation of the network and its performance are the key to its operation. With this documentation, network performance baselines can be achieved. Also, this documentation can aid in connecting other You Decide Company branch offices to the Cleveland Branch office's network. The network implementation, security and monitoring policies should be used as templates to design, implement and maintain the network at You Decide Company's corporate headquarters in Pittsburg, PA. These procedures and secure tunneling to branch offices nationwide will be the creation of an efficient and cost effective corporate network for the You Decide Company.

References

Vachon, Bob & Graziana, Rick.(2008). Accessing the WAN. (pp. 526-560). Indianapolis, IN: Cisco Press.

Network Monitoring PDF. (Nov. 15,2001). University of Utah Office of Information Technology Network Monitoring Policy. Retrieved from: http://it.utah.edu/leadership/policies/NetworkMonitoring.pdf

Brandenburg, Michael. (no date). How to Set a Network Performance Baseline for Network Monitoring.

Retrieved from: http://searchnetworking.techtarget.com/How-to-set-a-network-performance-baseline-for-network-monitoring

6. Network Monitoring Policy

Potter, Ronald. (no date). ITIL -- What Network Managers Need to Know. Retrieved from:

http://searchnetworking.techtarget.com/tip/ITIL-What-network-managers-need-to-know

International Foundation for Online Responsibility. (no date). Policy. Retrieved from:

http://www.iffor.org/policy

InfoSec. (no date). Technical References Guidelines & Standards. Retrieved from:
http://www.infosec.gov.hk/english/technical/guidelines.html