GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

John Lee
4/11/04 – Creating a Router / Firewall Security Policy
Sans GSEC Practical version 1.4b option 1

Introduction 2
The Team Concept 2
Classifying network infrastructure components 2
Common Services and features for all devices 4
Password policies 4
Common Services permitted by classification and type of device 4
Acceptable Routing Policies 5
Router / Firewall command policy 5
Management Networks 5
Configuration and diagram censuring 6
Media handling 7
Change Management 7
Asset management 7
Physical security 8
Incident escalation 8
Education 9
Periodic Review 9
Tying it all together 9
References: 12

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

With threats appearing on a daily basis, it is of growing concern for the Information Technology manager / security practitioner to be able to formulate an enterprise security policy that covers all the individual aspects of security. "A policy is a guideline or directive which indicates a conscious decision to follow a path towards a specified objective"(SANS p. 339). This document is intended to focus the reader on the specified objective of router / firewall security. This document has been written as a guideline for an individual organization to author and implement its own router / firewall security policy.

This document begins by emphasizing the necessity of group education and participation in creating and implementing a security policy. Classifying routers and firewalls based on the level of trust necessary to secure the network can simplify policy management. Password policies help to establish a minimum level of acceptable administrative passwords. Principles for minimizing security compromises are referenced throughout this document. Change management controls are discussed in this document as a tool to maintain compliance with corporate policies. A security policy is a living document and as such is subject to revisions. As part of the committee approach, the committee should be formed as a permanent group that will review and maintain the policy. It should be noted that the author's area of expertise is primarily on Cisco equipment, and the examples used in this document will reflect that expertise. Although this document will illustrate examples using Cisco equipment, the concepts are vendor-neutral and can usually be adapted to different vendor equipment.

The Team Concept

One of the most important aspects of implementing a security policy is the education of the target audience. In the case of a router / firewall policy, a key group is the network administrative staff. These are the individuals that will be responsible for enforcing the policy. It is a good idea to get the administrative staff involved in the creation of the policy. One possibility is to form a security policy group. Include the administrative staff and encourage their suggestions and comments. This will eliminate many questions and increase the acceptance of the policy when it is finished. A short meeting on a regular basis with assignments to each member of the group will help to keep interest during the creation phase of the policy. Each meeting should focus on one or two topics to keep the meetings concise and properly focused. Prior to forming the committee, it is a good idea to get the backing of senior management on the need for a security policy. Senior management's role will be critical when enforcing compliance of the policy. Budgets may need to be expanded in order to finance new technology to enforce the new security standards.

Classifying Network Infrastructure Components

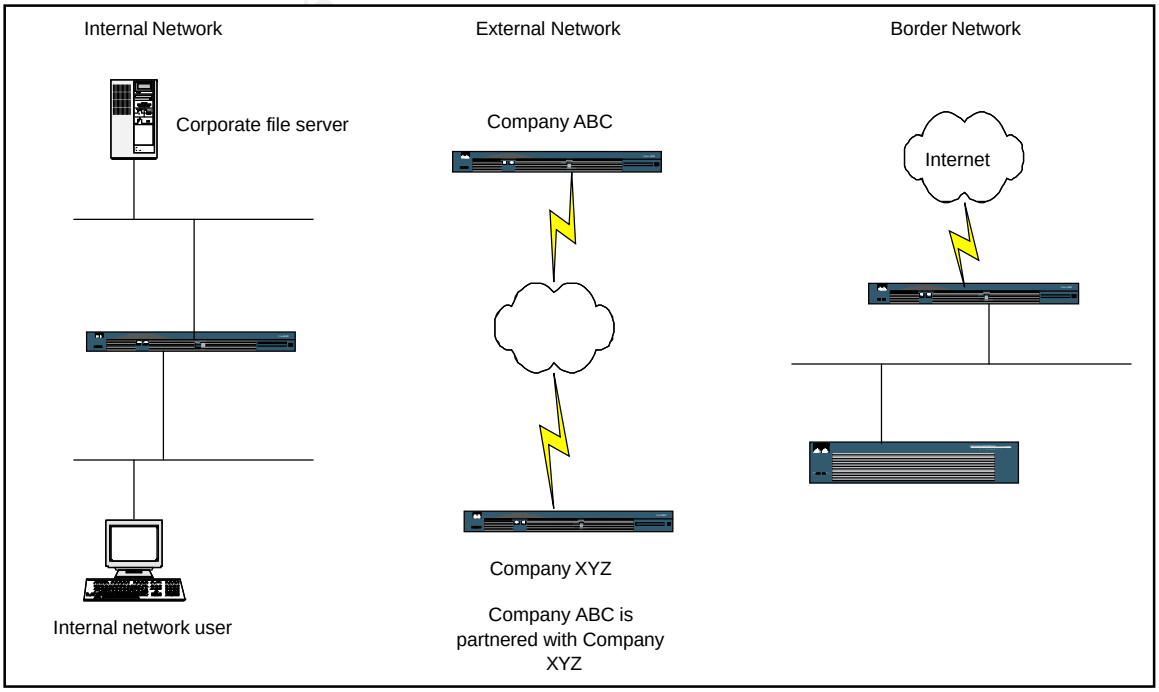
Identifying network assets is a vital step in understanding what needs to be protected. In today's complex networks, many routers, switches and firewalls are

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

connected together to make up the fabric by which data flows. One method of identifying network assets is to perform a physical inventory of all network equipment that falls into the scope of the policy. Once all devices have been inventoried, an analysis of their functions on the network needs to be conducted. The processes of categorizing network infrastructure components involve analyzing the component's connections to determine the level of trust between the two or more entities that the component connects. Once the analysis has been completed, a classification label is assigned to groups of devices that have the same level of trust. Our example uses a router connecting two networks. Classifying the router would involve the analysis of the networks that the router is connected to. If a router is connected to route internal networks (networks that are located within the company and under the control of the same network staff), we can classify this type of router deployment as Internal. Usually internal networks require the least amount of security due to the high level of trust between internal networks.

A second classification is the External classification. An external classification denotes that the device is used to connect two or more networks that are not under the control of the same network group, but have an established level of trust between the networks. An example of this would be a business partner or business-to-business intranet. Business partnerships often help to determine the level of trust between networks. The third classification we will discuss is the Border classification. Citing our example above, a Border device connects networks that are external, but with very little trust between the networks. Common examples are the devices that connect a corporate network to an Internet Service Provider. Classification of infrastructure devices is vital to establishing a security policy. It is up to the IT department or security officer of an individual company to determine the classifications and the level of trust assigned to each classification. Once the classifications are clearly defined, they should be included in the security policy to provide a consistent definition should the need arise.

Figure 1. Router configurations



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Common Services and Features for All Devices

Within the security policy for routers and firewalls, common services should be included in a common services section. This section includes the bare minimum of device configuration; these can include but are not limited to:

1. Login banners. Login banners are useful to inform potential users that use of the login is only for authorized users. “From a security, rather than a legal, point of view, your login banner usually should not contain any specific information about your router, its name, its model, what software it's running, or who owns it; such information may be abused by crackers.” (Cisco[1])
2. Logging. Logging can be useful for forensic analysis as well as for audit purposes. A policy should specify the type of logging to be performed.
3. Time syncing. All network clocks should be synced to a common time source. This is useful when performing forensic analysis of logs that were created by different devices. Correlation of events is made simpler when the times of the events are all in sync.
4. Authentication, Authorization and Accounting. The method for implementing an AAA model to secure the device should be included in the common services for all devices. This will help provide a consistent method from a management perspective. In the case of forensic investigation, a AAA model will help trace any administrative command entered by network engineers.

Password Policies

Although password policies can be grouped in the common services section, it is an important subject that merits its own section. This section should focus on the administrative passwords that are necessary to manage and maintain the equipment. An example of a password policy guideline is located at http://www.sans.org/resources/policies/Password_Policy.pdf
Specify a minimum password length as well as the format. For example, “a password can be no less than 8 alphanumeric characters”, or “a password can be 2 words with a minimum of four characters separated by punctuation” (“Cable:phoNes”). If two-factor authentication is available, specify the need to use it on all routers / firewalls. The policy should address who is responsible for changing passwords and the frequency that the changes should occur. Educate the staff on proper password handling. Passwords should never be written down or shared.

Common Services Permitted by Classification and Type of Device

Once classifications are determined, devices that fall into a classification may be grouped by type within each classification. For example: Internal routers, External routers, Border firewalls etc… Each classification and device type

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

should be configured with a similar feature set to ensure a consistent adherence to the security policy. Services that are common to each category in a classification can be group together to include either services expressly permitted or services expressly denied. This is up to the author of the policy to decide on which stance to take with common services. An example of a service common to many devices is SNMP. It may be necessary to restrict SNMP on Border devices to prevent rogue SNMP queries originating from foreign networks. This can be written into the policy for all Border devices to expressly deny SNMP from foreign networks. A list of services should be compiled and analyzed for necessary use and existing vulnerabilities. Determining and disabling unused services is critical to high- level security and plays an especially important task in managing networks with low levels of trust (External and Border classifications). Reference http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#possibly_unnecessary (Cisco[2]) for additional information on unnecessary services.

Acceptable Routing Policies

Acceptable routing policies can be grouped by the classification labels of the router / firewall. Acceptable routing policies describe what routing protocols are allowed or denied. Dynamic vs. Static routing, Interior vs. Exterior routing protocols can all be specified in this section. Tunneling protocols can be specified in this section to provide provisions for VPN sessions. Key lengths, encryption policies should be researched and an acceptable combination for both included in the policy. This section can be expanded to include acceptable firewall rules. It may be expressly denied to allow ICMP to pass through any firewall in the company. Features of the firewall that are acceptable can be noted here, but many times with firewall configuration, the policy will take the expressly denied posture.

Router / Firewall Command Policy

Depending up on how in-depth the security policy is, appropriate configuration and diagnostic commands my need to be documented. These are usually reserved for administrative personnel. If the organization has several levels of technical support staff, commands may need to be restricted on a user access level model. On Cisco equipment, this can be accomplished by using an AAA model on each managed device combined with a TACACS+ server (Terminal Access Controller Access Control System+) Please see: http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_configuration_example09186a0080093c7c.shtml (Cisco[3]) for a configuration example and explanation.
If these commands need to be restricted for different technical levels, it is a good idea to include a section in the security policy that defines the restrictions.

Management Networks

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Protection of network access devices are often too narrowly focused on preventing unauthorized outside access (access from foreign networks). Unauthorized access from an inside source is just as important to protect. Whether intentional or unintentional, the possibility of an inside originated compromise is present. Restricted inside access to interfaces of network components is a preventative measure often overlooked when securing a network. Although this subject should be integrated into the design phase of a network, it may have been missed with legacy designs. Separate management networks should be created to allow only authorized personnel access to network interfaces of all routers, switches and firewalls. A separate management network redefines which interfaces are used for management of the devices. The IP addresses assigned to the management interfaces are often not part of the mainstream corporate network, and do not show up in routing tables. The management network can be created using a loopback interface that is internal to the device. Common access to the interface is denied, and all configuration is restricted to the loopback interface. This concept prevents a common network user from successfully connecting to the interface while allowing network administrators the ability to manage devices remotely. The security policy should state who is allowed management access to network devices. If the corporation adopts the concept of a separate management network, a section in the policy should describe the management network. Common network services should include a section on the configuration of each network device for the management network.

Configuration and Diagram Sanitizing

In the normal course of maintaining a network, it is often necessary to obtain vendor support to help in fault isolation. Many times the vendor's technical support staff will request copies of equipment configurations. It is good practice to remove any information from the configurations that are deemed sensitive. This is especially important for equipment that is publicly accessible. Dummy IP addresses should be substituted for publicly routable addresses. Passwords (even if hashed) should be removed and replaced with a line that indicates the password was removed. When network technicians troubleshoot with the vendor's support, both parties should use the sanitized configuration. This practice should also apply to network diagrams. Network diagrams are used as a visual aid to understanding network traffic flow. Imagine if these diagrams fell into the wrong hands. In the wrong hands, a network diagram gives a potential attacker a "roadmap" to the entire network. A good practice is to create a sanitized version of the network diagrams. The sanitized version would not include any sensitive information that would compromise security if they fell into the wrong hands.

There are times when sales departments ask the IT department to supply technical drawings for presentations or customer contracts. The practice of using sanitized documents shuts down another avenue where valuable network information can be compromised. The security policy should clearly state the procedure for handling sensitive configurations and diagrams. In environments

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

that have frequent visitors (outside service personnel, customers, business partners) the organization may feel it necessary to prohibit displaying sensitive configurations or diagrams in high traffic areas. This would especially apply to Network Control Centers where diagrams may be displayed for technical use.

Media Handling

When configurations are transported using magnetic media, a procedure should be included to address the proper handling of the media. Many times network technicians need to transport configurations from devices during the course of troubleshooting a problem. Leaving a floppy diskette unsecured is another way that sensitive information can be compromised. It is important to ensure that when finished, the media that was used is properly accounted for. The same principle applies to printed material. Printed configurations and network diagrams can also be a source for a security compromise. The procedure should address the approved method for securing the information or destroying it.

Change Management

Change management is becoming a necessity due to increasing regulations and audit compliance. Change management allows an IT manager and Security Officer to effectively track network changes. Depending on the size of an organization, a change management process can be a simple form filled out by requestors of changes or a larger electronic system driven by a database. Both small and large systems tracks requests and approvals. Change Management also serves as a good starting point in the event that recovery of services become necessary. With all changes documented, it simplifies the recovery process and ensures that critical network data flows are not left out.
A simple way to build a change management request form or application is to answer the 5 W's. Who is requesting the change? What configuration is required to make the change? Where is the change to be made? When is the changed required? Why is the change necessary? As above with the change management process, it is important to determine what happens once a request has entered the system. Once again answer the 5 W's to establish roles within the policy. Who is authorized to approve and make changes? What changes are permitted? Where can the changes be made (is remote management allowed?)? When can changes be made (is there a service outage window?)? Why are the changes being made?

Asset Management

Asset management plays an important role in developing a secure router / firewall policy. In environments where devices are deployed in multiple locations, tracking assets becomes more critical. Physical security is dependant upon the successful implementation of an asset management policy. Network access devices must be accounted for. This concept is illustrated in the case of cold spares. A cold spare router or firewall may be put on a shelf or in a cabinet for emergency use. Many times these cold spares contain partial or full configurations that mirror the deployed device. If the device is misplaced or

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

stolen, a valid configuration becomes lost and a potential intruder may gain valuable insight into a company's network. Depending on the number of devices tracked, asset management can be in the form of an electronic document such as a spreadsheet, or a larger database driven application. It is important to include a policy for asset management that can easily be audited on a scheduled basis. Simply knowing that a device "should be located at…" is not enough. A verification process should be included in the policy and performed on a scheduled basis. This will also aid in keeping configurations up to date. The policy should include how new equipment enters the network as well as how end of life equipment is removed from the network. Include in the asset management policy, what areas within the company are authorized to perform the addition, modification or removal of equipment and the procedure for updating the asset management system.

Physical Security

Physical security should be addressed in the security policy. It is just as important to secure the network devices physically as well as logically. Address physical security in terms of providing a secure environment where the equipment is installed. This may include locks and keycard entry systems. If either system is in use, specify who is allowed access and the times that they are allowed access. It may be occasionally necessary to allow a vendor into the environment for repairs. In this case, a formal sign in / sign out process should be enforced. This may already be enforced for the entire building, and if that policy is deemed as sufficient, reference the procedure in the security policy. Include references to existing procedures regarding physical security. Depending on the overall security of the corporation, the use of equipment removal forms may be necessary. It is also a good idea to reference the change management section regarding who is allowed to move equipment. Include who is allowed physical access to all equipment. Logical security is simplified when physical security has been addressed. On certain devices such as Cisco routers, there are published procedures to reset the password. This procedure is dependant upon having physical access to the router. The failure to provide proper physical security could put the logical security at risk.

Incident Escalation

Incident response is another area necessary in a security policy. It is important to identify who is responsible when an incident occurs. Events such as a security compromise are generally handled by a CSIRT (Computer Security Incident Response Team). According to CERT in their CSIRT FAQ, "Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it will be critical for an organization to have an effective way to respond." If the corporation has an existing CSIRT, the security policy should refer to the CSIRT manual for security incident handling. If the corporation does not have the resources for a CSIRT manual, the security policy can attempt to fill in the gaps necessary for security response. Other incidents that fall outside the scope of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

security can also be identified within the policy. The security policy should include the roles necessary to respond to different incidents. In addition to role assignment, an escalation chart should be included. An escalation chart shows the path of escalation based on timed intervals. This shows that after a predetermined amount of time if the incident is not resolved, another tier of support needs to be notified and activated. This ensures that incidents receive the proper amount of attention in a timely manner. Detailed procedures on how each type of incident should be handled can be included in the security policy. "It is critical for an organization to determine its defense posture prior to an incident. This posture will dictate the organization's procedures and critical first steps when an incident occurs" (Mandia, Procise, &Pepe p.54)

Education

Education plays an important part in establishing a new security policy. "Training for employees is key. This includes everyone, engineering to janitorial. " (Riverstone). By educating the staff on the security policy it helps to make everyone more security conscious. Education on the topics of the new policy will also help in alleviating potential friction generated between co-workers. For example, prior to the implementation of a security policy, a network change could be accomplished in a relatively quick amount of time, while after the policy has been implemented, the same network change may take one business day. This could be due to new change management process dictated within the policy. The originator of the change may be more understanding if he /she were advised of the new policy and more importantly why the policy has been put in effect.

Periodic Review

As stated in the opening paragraph, the security policy is a living document. As technology changes, the policies that govern the secure operations of those devices will need to change. With the authoring committee already established, it may be a good practice to keep the committee together as a periodic review panel. This panel should bring any relevant changes in technology or policy to the scheduled meetings. Most of the time a quarterly review is sufficient.

Putting It All Together

To tie all of the sections covered in this document together, we will generate a task list used to create a framework of the secure router / firewall policy. As previously discussed, depending on the size of the enterprise, some sections may not apply and may be omitted.

1. Discuss the importance of a security policy with Senior Management. Obtain official approval for the creation of a secure routing policy.
2. Form a task force or committee to create a security policy. Remember to include all members of the staff that will have direct impact on the policy. Set regular meetings with specific agendas and assign take away tasks as necessary. These meetings should be short and targeted towards a specific goal per meeting.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Collect information regarding all of the routers / firewalls deployed within the enterprise. Include all connections to remote sites.
4. Analyze the functions of all routers and firewalls gathered during step 1. Create classifications for each of the functions. As suggested in the section above, Internal, External and Border classifications may fit the organization's types of connectivity.
5. Assign a desired security level to each classification (High, Medium or Low). Include a general description of each classification within the policy
6. Decide the position that the policy will take. Choose either the expressly permitted or expressly denied posture.
7. Decide on the common services permitted / denied for all deployed devices. This area may be a good place to put an acceptable password policy under a subheading. Include all services that are common to all devices.
8. Create the common services per security classification sections. Decide on what services are permitted / denied based on the level of security that is necessary per classification.
9. Create an acceptable routing section for the policy. This section specifies routing that is permitted / denied on each classification based once again on the level of security defined in each classification. If firewalls are deployed, include a section on acceptable firewall rules.
10. Discuss with the committee the necessity of having a separate management network for all devices. Depending on the available resources both hardware and staff technical ability, this section is considered optional.
11. Create a section for sensitive media handling. Include the sections from above that discuss sanitizing configurations / diagrams and proper media handling.
12. Discuss change management. Create a section on change management. If this does not exist within the company today, discuss with the committee the need for change management.
13. Create an asset management section. Once again, if not already established within the company, this makes an excellent venue to get an asset management program started.
14. Analyze the current state of physical security within the enterprise. Make changes where possible to enhance physical security. Simple door locks or cabinet locks can quite often provide deterrence against theft.
15. Create an incident response section. Depending on the size and availability of resources, the company may already have a CSIRT (Computer Security Incident Response Team). Include the incident escalation chart.
16. Assign the committee the task of creating an education program to educate the network users on the security policy.
17. Prepare a schedule to periodically review the policy, looking for outdated issues or inclusion of new subjects.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

By using the 17-step checklist above, an organization can put together a basic framework of best practices to include in the security policy. This document represents one way in which a security policy can be created. Each organization differs in its interpretation of security and by using a best practices system as outlined above, organizations can create a policy tailored to their specific needs.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

Cisco Systems
[1]Improving Security on Cisco Routers; Document ID: 13608;
http://www.cisco.com/warp/public/707/21.html

[2]Improving Security on Cisco Routers; Document ID: 13608;
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#possibly_unnecessary

[3]Basic TACACS+ Configuration Example
http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_configuration_example09186a0080093c7c.shtml

SANS
Password Policy
http://www.sans.org/resources/policies/Password_Policy.pdf

Sans Security Essentials book
Chapter 8 Defining a policy pp339

CERT (Computer Emergency Response Team)
Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)
http://www.cert.org/csirts/csirt_faq.html

Mandia, Kevin; Procise, Chris; Pepe, Matt. “Incident Response & Computer Forensics” 2003:p54

Riverstone
Riverstone Security and Operations Guide
http://www.riverstonenet.com/support/rso/managing.shtml

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.