1.4 Vulnerability Analysis
1.4.1 Policy review

Before adding new security solutions to an existing network, the current state of the network and organizational practices needs to be identified to verify their current compliance with the requirements, and identify possible improvements and the potential need to redesign a part of the system, or to rebuild a part of the system from scratch to satisfy the requirements.

Policy Identification
If a security policy exists, the designer should analyze it to identify the security requirements, which will influence the design of the perimeter solution. Initially, two basic areas of the policy should be examined:

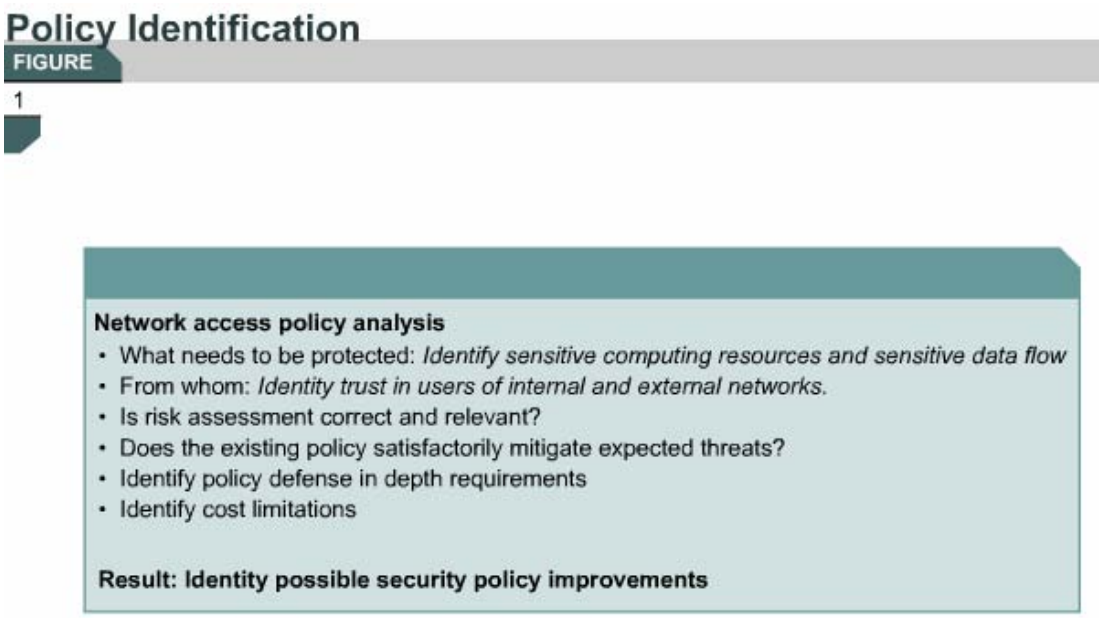
The policy should identify the assets that require protection. This will help the designer provide the correct level of protection for sensitive computing resources, and identify the flow of sensitive data in the network.
The policy should identify possible attackers. This will give the designer insight into the level of trust assigned to internal and external users, ideally identified by more specific categories such as business partners, customers of an organization, outsourcing IT partners.

The designer should also be able to evaluate if the policy was developed using correct risk assessment procedures. For example, did the policy development include all relevant risks for the organization and not overlook important threats? The designer should also re-evaluate the policy mitigation procedures to determine if they satisfactorily mitigate expected threats. This ensures that the policy, which the designer will work with, is up to date and complete.

Organizations that need a high level of security assurance will require defense-in-depth mechanisms to be deployed to avoid single-points-of-failure. The designer also needs to work with the organization to determine how much investment in security measures is acceptable for the resources that require protection.

The result of policy analysis will be:

The evaluation of policy correctness and completeness
Identification of possible policy improvements, which need to be made before the securityimplementation stage



1.4 Vulnerability Analysis
1.4.2 Network analysis

There are many industry best practices, tools, guides, and training available to help secure network devices. These include tools from Cisco such as AutoSecure and Cisco Output Interpreter, as well as numerous web resources. Third party resources include the U.S. National Security Agency (NSA) Cisco Router Security Recommendation Guides and the Center for Internet Security (CIS) Router Audit Tool (RAT) for auditing Cisco router and PIX Security Appliance configuration files.

Cisco AutoSecure
Cisco AutoSecure is a Cisco IOS Security Command Line Interface (CLI) command.

AutoSecure

FIGURES

1 2 3 4 5 6

Command	Description
`auto secure [management | forwarding] [no-interact]`	• Secures the management and forwarding planes of the router. • **`management`** - Only the management plane will be secured. • **`forwarding`** - Only the forwarding plane will be secured. • **`no-interact`** - The user will not be prompted for any interactive configurations.
`show auto secure config`	• Displays all configuration commands that have been added as part of the AutoSecure configuration.

AutoSecure enables rapid implementation of security policies and procedures to ensure secure networking services. It enables a "one touch" device lockdown process, simplifying the security configuration of a router and hardening the router configuration. This feature simplifies the security process, thus lowering barriers to the deployment of critical security functionality.

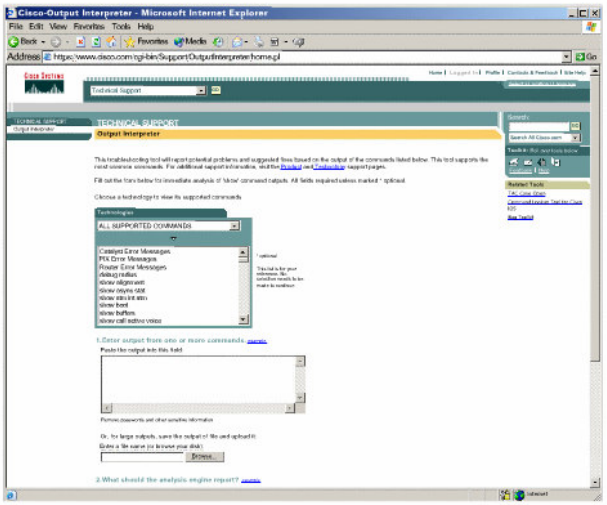
Cisco Output Interpreter

The Cisco Output Interpreter is a troubleshooting tool that will report potential problems by analyzing supported show command output.

Output Interpreter

FIGURES

1 2 3 4 5 6



The Output Interpreter is available at the Cisco website to users with a valid Cisco Connection Online (CCO) login. Output Interpreter supports the following functionality:

show command outputs from a Router, Switch or PIX Security Appliance. A list of supported show commands is available at the Output Interpreter site.

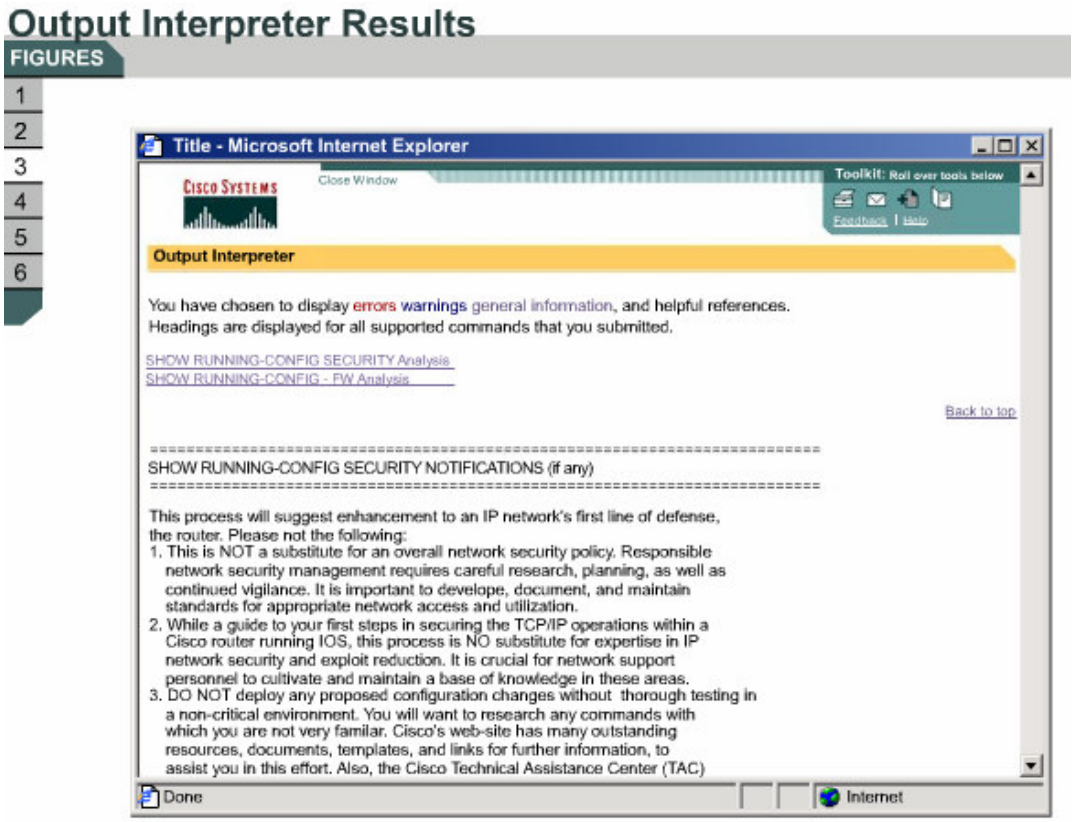
Error Messages generated by a Router, Switch or PIX Security Appliance. The Error or Log Messages can be copied and pasted from a Router, Switch or PIX Security Appliance into the Output Interpreter.

Decodes and analyzes a Router or Switch stack trace for any possible bugs. Copy and paste the show version command output followed by Traceback or Stack Trace and Alignment data.

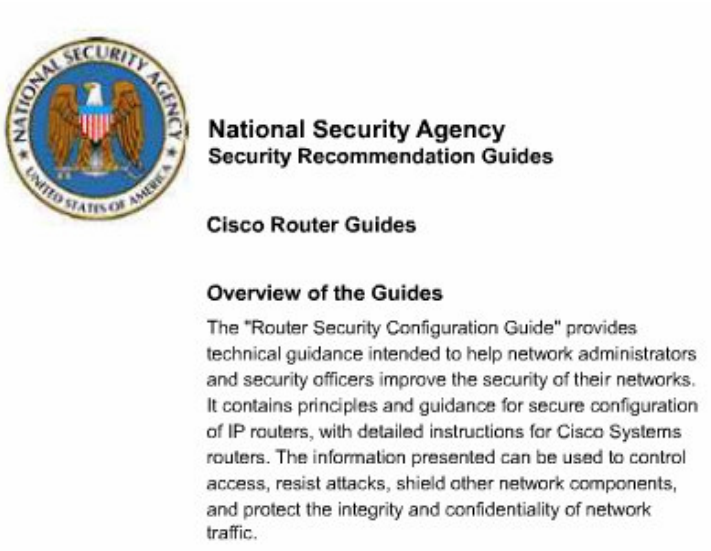
Is able to convert the apply, conduit, and outbound statements of a PIX Security Appliance configuration to equivalent access-list statements. Copy and paste show tech-support or write terminal command output of the PIX Security Appliance.

Decodes and analyzes the Configuration Register. Copy and paste the show version or show tech-support command output into the Output Interpreter.

Figure 3 shows an example of the output of the Output Interpreter.



National Security Agency (NSA) Cisco Router Security Configuration Guides
The Router Security Configuration Guide (RSCG) contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers.



The RSCG was used extensively in the development of the Cisco Router Security course. This guide was developed in response to numerous questions and requests for assistance received by the National Security Agency (NSA) System and Network Attack Center (SNAC). The topics covered in the guide were selected on the basis of customer interest, community consensus, and the SNAC's background in securing networks. The RSCG is a large, detailed, yet readable and accessible document. It is supplemented with an Executive Summary Card, a quick checklist for securing your Cisco router.

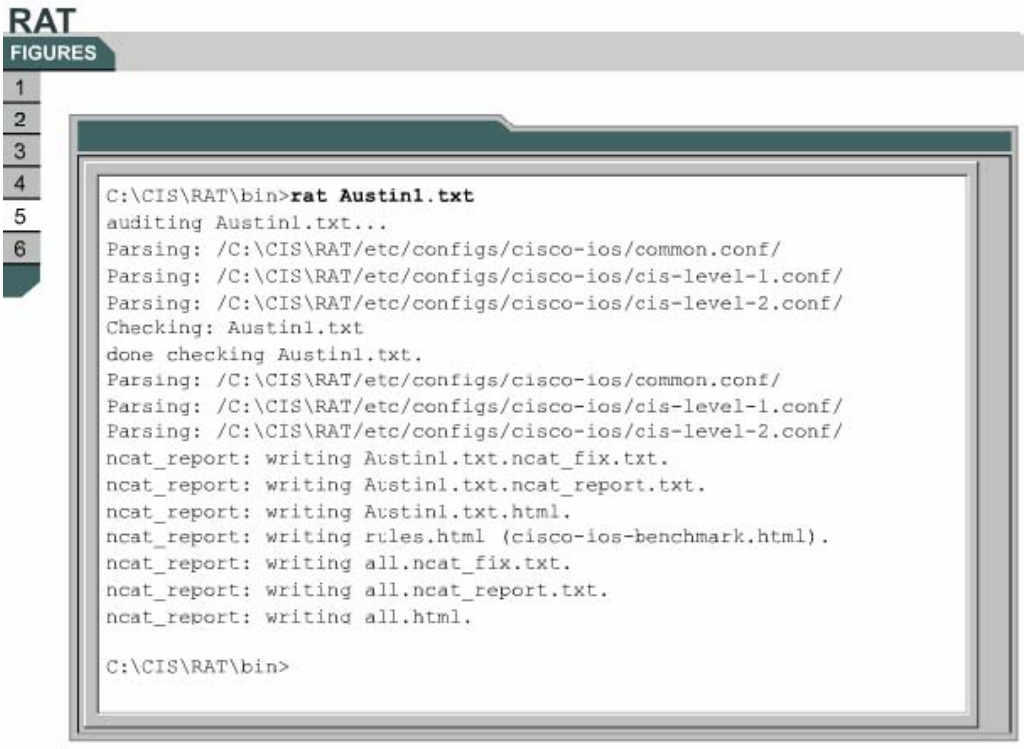
Routers direct and control much of the data flowing across computer networks. The RSCG provides technical guidance intended to help network administrators and security officers improve the security of their networks. Using the information presented here, you can configure your routers to control access, resist attacks, shield other network components, and even protect the integrity and confidentiality of network traffic.

The goal for this guide is a simple one, improve the security provided by routers on US Government operational networks.

The RSCG document is only a guide to recommended security settings for Internet Protocol (IP) routers, particularly routers running Cisco Systems Internet Operating System (IOS) versions 11 and 12. It is not meant to replace well-designed policy or sound judgment. The guide does not address site-specific configuration issues. Care must be taken when implementing the security steps specified in this guide. Ensure that all security steps and procedures chosen from this guide are thoroughly tested and reviewed prior to imposing them on an operational network.

Cisco Router Audit Tool (RAT)

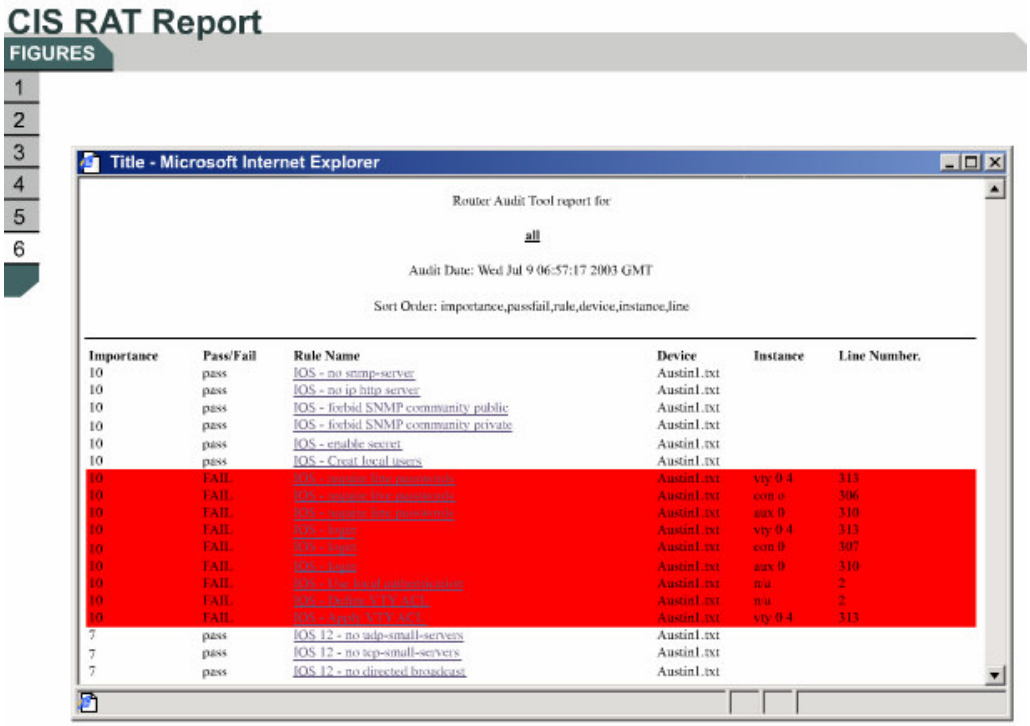
The CIS RAT is based on the CIS Benchmark for Cisco IOS Routers, a consensus-based best practice guideline for hardening Cisco routers. The version 2.2 of the RAT tool can be used to score both Cisco IOS Routers and PIX Security Appliances. The RAT is available for the Windows or UNIX operating systems. A sample RAT output is shown in Figure 5.



The RAT downloads configurations of devices to be audited (optionally), and then checks them against the settings defined in the benchmark. For each configuration examined, it produces a report listing the following:

A list of each rule checked with a pass/fail score.
A raw overall score.
A weighted overall score (1-10).
A list commands that will correct problems identified.

The RAT produces a composite report listing all rules (settings) checked on all devices, as well as an overall score, and recommendations for improving the security of the router, as shown in Figure 6.



1.4 Vulnerability Analysis
1.4.3 Host analysis

The hosts that are on the network need to be taken into consideration when designing a network security solution. Determining the role in the network of each host will help to decide the steps that will be taken to secure it. The network could have many user workstations, as well as multiple servers that need to be accessed from both inside and outside of the network.

The types of applications and services that are running on the hosts need to be identified, and any network services and ports that are not necessary should be disabled or blocked. All operating systems should be patched as needed. Antivirus software should be installed and kept up to date. Some servers may be assigned static routable IP addresses to be accessible from the internet. These hosts in particular should be monitored for signs of malicious activity.

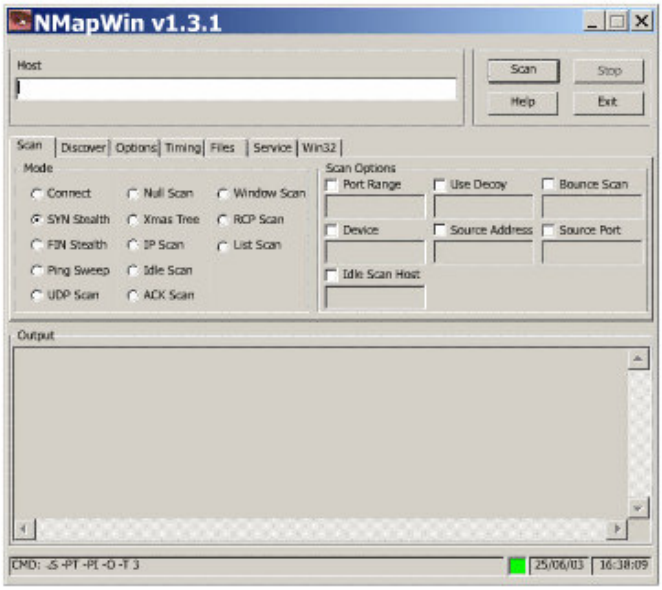
There are many tools that are available to test host security. Most tools have been developed on a UNIX or Linux platform, and some of them have now been ported to other operating systems. Two of the most common tools are described below:

Network Mapper (Nmap) – Nmap is a very popular free tool used for security scanning and auditing. It can rapidly perform a port scan of a single host or a range of hosts. Nmap was originally written to be run on UNIX systems, and it is now available for use on Microsoft Windows platforms .

Nessus – Nessus is a vulnerability scanner that is available for UNIX and Microsoft Windows platforms. New vulnerability testing capabilities can be added to Nessus through the installation of modular plugins. Nessus includes a built in port scanner, or it can be used along with Nmap. Once the Nessus scan is finished, a report is created. This report displays the results of the scan and provides steps that can be taken to mitigate vulnerabilities.

NMAP for Windows

FIGURE 1



1.4 Vulnerability Analysis
1.4.4 Analysis tools

There are many tools available to help to determine vulnerabilities in endpoint devices, such as network hosts and servers. These tools may be obtained from either the company that creates the operating system or a third party. In many cases these tools are provided for free.

Knoppix-STD
Knoppix Security Tools Distribution (STD) is a Linux LiveCD distribution that contains many valuable security tools. The LiveCD is a bootable CD-ROM that contains the Linux operating system, along with software applications, that can be run from memory without installation on the hard drive. After the LiveCD is ejected from the CD-ROM drive, the system can be rebooted to return to the original operating system. Knoppix STD contains many useful features, such as:

- encryption tools
- forensics tools
- firewall tools
- intrusion detection tools
- network utilities
- password tools
- packet sniffers
- vulnerability assessment tools
- wireless tools

There are many additional versions of LiveCDs available. If one distribution does not support a particular system or piece of hardware, it may be necessary to try another distribution. Most LiveCD releases are available as free downloads that can be burned to a CD by the end user.

Microsoft Baseline Security Analyzer
The Microsoft Baseline Security Analyzer (MBSA) can be used to scan hosts running Windows 2000, Windows XP, and Windows Server 2003 operating systems to determine potential security risks. MBSA scans for common system misconfigurations and missing security updates. MBSA includes both a graphical and command line interface that can perform local or remote scans. After a system scan, the MBSA provides a report outlining potential vulnerabilities and the steps required to correct them. This tool is available as a free download from Microsoft.

Summary

This module introduced the needs, trends, and goals of network security. The exponential growth of networking has lead to increased security risks. Many of these risks are due to hacking, device vulnerabilities, as well as improper uses of network resources. Awareness of the various weaknesses and vulnerabilities is critical to the success of modern networks. Security professionals who can deploy secure networks are in high demand.

The four primary threats to network security include unstructured threats, structured threats, external threats, and internal threats. In order to defend against threats, an understanding of the common methods of attack must be established, including reconnaissance, access, denial of service, and malicious code.

Responses to security issues range from ignoring the problem to excessive spending on security devices and solutions. Neither approach will be successful without a good, sound policy and highly skilled security professionals.