Global Information Assurance Certification Paper

Perimeter Filtering in a university setting

Elizabeth Mackenzie, Director System Security, Access and Help Services
University of Delaware
9/11/2000
betsy@udel.edu
(302) 831-1975

Introduction

A University faces tough choices in deciding how and what to filter at the network borders. There is a trade-off between performance of the network and support of the open education and research environment on the one hand and system security on the other. Central system administrators at the University of Delaware believe that minimal filtering should be done at the border.

This paper will explain the risk assessment and security policy that led to this decision. The paper will defend the position of minimal border filtering by explaining the requirements of an open environment in an educational setting. It will describe the configuration of our router and how we implement ingress/egress filtering. Finally, the paper will suggest filtering implementation for departmental servers to protect individual host machines.

Risk Assessment

The University of Delaware uses a CISCO 7507 router to connect to the Internet. The router is connected to Voicenet through fast Ethernet full duplex and Abilene via OC-3 packet over sonnet (pos). The router also provides connections to the old backbone via ATM OC-3 and the new backbone via gigabit Ethernet. The configuration of the CISCO router is, in effect, our firewall.

Before we can determine what level of security is sufficient we must assess the risks associated with the current implementation. A complete security risk assessment is beyond the scope of this paper, this assessment is restricted to the security of the border router. The method used was developed by A C Lynn Zelmer, PhD; and is described on the CQU web site.

Zelmer's method includes 4 steps; definition of assets, threat assessment, risk assessment and recommendations.

Assets

The assets at risk from targeted attacks against the network using the border router's current filtering rules include routing services-access to the Internet,

access to central servers and data stored on those servers. There are roughly 30,000 accounts on the central servers. Each user is allocated 4M. The amount of data at risk is potentially 120GB.

Threat assessment

Tools are readily available that allow even novices to attack and possibly penetrate network defense. Potential agents range from sophisticated and talented programmers, to relatively inexperienced teenagers. These agents could potentially disclose sensitive data, modify or destroy data, or as a privileged user, the agent could take control of the central systems and/or deny service. Unauthorized users may use the resources to commit a crime, for instance violate copyright law. Some hostile intruders will steal accounts from which they launch further attacks on other sites.

The potential impact is serious. Data is backed up nightly. In the worst-case scenario, the maximum data loss would include files created or modified in the previous 24 hours. Our disaster recovery plan contracts with a vendor that can restore network connectivity either on-site or off, within a day, so network access would likely be lost for at most, one day.

Any serious breech of our network defense could cause long term consequences including, disclosure of sensitive data, perceived lack of security, harm to the reputation of the school and IT staff, and exposure to lawsuits.

Risk Assessment

The current configuration of the University's border router prevents IP spoofing of a Delaware address, blocks broadcast addresses, blocks most Netbios traffic, protects critical systems, provides access to the web and denies access from known hostile hosts.

The University network is vulnerable to attack through the border router. The router is not configured to block any specific ports. The central servers use TCP wrappers, but the hosts.allow file reads ALL:ALL.

Admittedly, the risk of malicious packets making it through the router into the University network is very high. But, the router is not the last line of defense, each host can protect its own perimeter with much more restrictive filtering. If we consider a network with limited filtering at the border router, but secure and hardened hosts, the risk becomes very small.

Security Policy

As a teaching and research institution, the University of Delaware must provide an open environment. As Dan Grim, Executive Director, Network Systems and

Services said, “It is very difficult, if not impossible, to limit access in a manner that suits everyone's needs and desires. I would like to think that we run the network in a similar manner to the Library in that we make available anything that has any legitimate academic use and make no pre-emptive decisions about what that might be.”

Collaborative research requires sharing information in many ways. For example, several departments on campus were using Netbios for support and debugging. When we attempted to filter Netbios traffic at the perimeter, we found we had cut off access for legitimate users. Another example noted by Steven Vaughn-Nichols in his article “Choose the Best Security Bricks for a Firewall” is Real Audio. Many router configurations routinely blocked UDP traffic before Real Audio was widely used. A system administrator cannot anticipate all future uses of network technology.

The university has a need for extremely high-speed access. At these high speeds network performance declines rapidly as filtering rules are added

As a teaching institution we believe students should have access to the Internet and the opportunity to experiment as they learn. Obviously we don’t encourage hostile behavior, but teaching and research often require liberal access. A University Information Technology office’s first priority is to provide computing resources to students and faculty and to encourage and foster research and collaboration. We cannot provide this if we adopt the philosophy of “block everything, permit on demand”.

Our strategy is to provide very minimal filtering at the network’s perimeter. Individuals and departmental system administrators are encouraged to implement their own personal firewalls to provide protection. This provides the freedom required by some faculty and students while protecting resources on the campus network.

Configuration

The 7507’s configuration file is very flexible and establishes complex rules for permitting or denying access to or from the University’s network. These rules are contained in the router’s access list and can permit or deny access based on protocol, port, type of service, (tos), source ip and destination ip. This set of rules is consulted before any packet is transferred.

The CISCO 7570 uses Cisco Express Forwarding (CEF) to improve performance. CEF is a scalable, distributed, layer 3 (network) switching solution. Previous routing procedures used a cached router table. This was an effective strategy when large flows across the network shared the same source/destination ip pair. Network traffic is now characterized by intensive web based applications

and interactive sessions. The new model uses a forwarding information base (FIB) and adjacency tables.

The FIB contains a mirror image of the forwarding information in the IP routing table is updated whenever the routing table changes. The FIB maintains next hop address information based on the IP routing table. The adjacency table lists adjacent nodes (i.e. nodes that can reach each other with one hop.)

The adjacency table holds Layer 2 (data link) next hop information for all of the FIB entries. CEF uses adjacency information to prepend Layer 2 addressing information. An adjacency table entry can be the null adjacency. The null adjacency drops packets and can be used to implement the system's filtering rules.

We identified the following set of rules to filter packets at the border router.

- prevent IP spoofing (Udel coming in)
- block broadcast addresses
- block Net Bios traffic (with exceptions)
- protect critical systems
- provide access to web
- deny access from known hostile sites.
- permit everything else

The syntax for the access list in the router configuration file is as follows:

```
permit/deny  protocol  source ip       destination ip  [tos/port]
```

Deny IP Spoofing

No packets coming into the University's network from outside the Udel domain should have a source IP containing our domain. The following entry denies access to a packet that is trying to spoof a udel address.

```
deny        ip        128.175.0.0 0.0.255.255        any
```

This line instructs the router to deny access to any packets that have a source IP beginning with 128.175. and any destination address.

Broadcast/Loopback adresses

A packet with a destination address that is the broadcast address will go to every host on the network. To prevent broadcasts (and possibly denial of service) we use the following

```
deny       ip          any              0.0.0.255 255.255.255.0
```

This line instructs the router to deny access to a packet from anywhere destined for the broadcast or loopback address.

Block Netbios

Last year we found enormous amounts of data flowing out of the University network from connections in dorm rooms. On investigation we determined that someone was systematically scanning the student connections looking for unprotected Windows shares. We have a very limited need for Netbios outside the network so we allow those few exceptions and deny all other Netbios traffic.

```
permit    ip       any      128.175.x.0 0.0.0.255
```
Permit netbios traffic to the x subnet.

```
deny      tcp      any      any      eq 139
deny      tcp      any      any      eq 138
deny      tcp      any      any      eq 137
```
Deny traffic in or out on tcp ports 137, 138 and 139

```
deny      udp      any      any      eq netbios-ss
deny      udp      any      any      eq netbios-dgm
deny      udp      any      any      eq netbios-ns
```
Deny traffic in or out on udp ports netbios-ss, netbios-dgm and netbios-ns

Protect Critical Systems

For those machines most critical to our operation, we deny all access. These include tape servers, the IVR system etc.

```
deny              ip              any             host 128.175.a.x
deny              ip              any             host 128.175.a.y
deny              ip              any             host 128.175.a.z
```
Deny all IP access to hosts x, y and z in the a subnet.

Provide access to the web

```
permit            tcp             any             host 128.175.a.w   eq www
permit            tcp             any             host 128.175.a.v         eq 443
```
Permit access to port 80 (www) on the webserver 128.175.a.w and permit tcp access on port 443 (https) to 128.175.a.v.

Recommendations for system administrators

Given the limited security afforded by the border router, departmental system administrators are advised to make their system as secure as possible. Take the "deny everything, permit on exception" approach.

System administrators are encouraged to install host perimeter firewalls. Host firewalls can block port scanners, protect against know exploits, log suspicious events and evaluate configuration. Firewall products can even be configured to page an operator on a specified event. Firewalls examine packets in both

directions so you can use a firewall to keep traffic from going out or to keep traffic from coming.

Departments must analyze their needs and work with established University security policies to determine their firewall needs.

There are several options available; Firewalls fall into four categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls. The following descriptions are adapted from the knowledgeshare website.

Packet filter firewalls are usually routers that apply rules to packets as they enter or exit the router. The University's border router is an example of a packet filter firewall.

Circuit level gateways monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computers through a circuit level gateway appears to have originated from the gateway. Use this option if you need to hide the IP's of your hosts from the world.

Application level gateways (a.k.a. proxies) route packets based on the application. An FTP packet must use the FTP proxy, a WWW packet must use the WWW proxy. If a proxy is not available for a particular service, the packet is not allowed. This is a good solution if you want to block all access to certain services. Proxies can filter application specific commands such as http:post and get, etc. This is an important feature not available on firewalls that work at lower levels. Application level gateways can also be used to log user activity and logins. Better security comes at a price though. Application level gateways will adversely affect network performance and host must be configured individually to work with the proxy.

Stateful multilayer inspection firewalls combine features of the other three types of firewalls. They filter packets at the network layer like a packet filter, determine whether session packets are legitimate like a circuit level gateway and evaluate contents of packets at the application layer like and application level gateway but they do not use proxies. Instead, these firewalls use sophisticated algorithms to process application layer data. Stateful multilayer inspection firewalls are expensive but they offer a high level of security, good performance and ease of use at the user end. They are however, very difficult to configure. Some argue that their complexity and the potential for mis-configuration makes them less secure than the other types.

References

Zelmer, A C Lynn, PhD;"Guidelines for Computer Security at CQU". Central Queensland University Computer Security Documents. 1996 URL http://www.cqu.edu.au/documents/compsec/guidelines/Assets (9/8/00)

Vaughn-Nichols, Steven Choose the Best Security Bricks for a Firewall ZDNet Developer, March 23, 1998 URL http://www.zdnet.com/devhead/stories/articles/0,4413,1600787,00.html (9/5/00)

Unknown, Firewall Q/A Vicomsoft Technology Limited Reference section, URL http://www.vicomsoft.com/knowledge/reference/firewalls1.html (9/8/00)

Grennan, Mark Firewall and Proxy Server HOWTO LDP Linux Documentation Project How-to Firewalls v0.80, Feb. 26, 2000 URL http://www.ssc.com/mirrors/LDP/HOWTO/Firewall-HOWTO.html (9/2/00)

CISCO Systems Inc. Technical Documentation, CISCO Express Forwarding Overview CISCO IOS Switching Services Configuration Guide. pp XC-21 – XC-26 Last updated Mon Jul 17 2000 URL http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt2/xcdcef.htm

Grefer, Roland and Jennifer Kolde "Host Perimeter Defense" Sans Security Essentials, Part 2. 7/6/2000

Kaufman, Charlie, Radia Perlman and Mike Speciner, "Network Security Private Communication in a Public World" 1995.