Global Information Assurance Certification Paper

SANS Security Baltimore 2001 GIAC Level Two
Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5e

Submitted by: Donald Guthrie
August 2001

Table of Contents

Assignment One: Security Architecture for GIAC Enterprises

The GIAC Enterprises infrastructure must provide necessary business services yet minimize security risks.

- The infrastructure must provide a web based e-commerce purchasing solution for customers.
- The infrastructure must provide access for GIAC Enterprises' suppliers.
- The infrastructure must provide access for GIAC Enterprises' international business partners.
- The infrastructure must provide secure remote access for GIAC Enterprises staff.

Customer Access: Customer's access to the e-commerce network will be via the Internet and web-based applications. Access to this network will be controlled by an application proxy firewall. The e-commerce network will be referenced to as the "*EC_GIAC Network*".

Secure Remote Access: The GIAC Enterprises staff will utilize a firewall based VPN solution for secure remote access to the GIAC Enterprises private corporate network, also via the Internet. This network will be referenced to as the "*PC_GIAC Network*". A packet filtering firewall will also be used to protect the PC_GIAC Network and positioned as a boundary device between the PC_GIAC Network and the supplier/partner network. This will implement a secondary protection scheme and exercise a layered security methodology for PC_GIAC Network.

Supplier/Partner Access: An additional VPN appliance will provide access and tunnel end points to the supplier and business partner network. This network will be referenced as the "*SP_GIAC Network*". Figure 1 reflects the GIAC Enterprises security architecture.

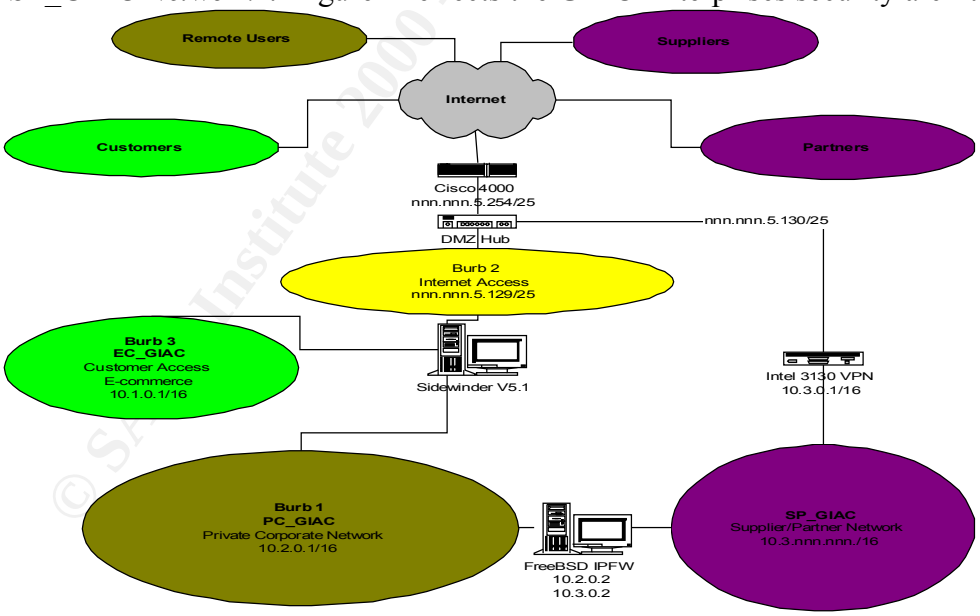


Figure 1

Cisco® 4000 Router with IOS 12.0

The GIAC Enterprises Cisco® 4000 router is the initial point of access and subsequently our first line of defense in the architecture. It will allow us to direct/restrict network traffic and services as well as compliment overall access control to our networks. This

will be accomplished by the implementation of access lists and filters via configuration of the Cisco® IOS. The 4000 although somewhat dated, should provide ample capability for our requirements.

Secure Computing Corp. SidewinderÔ Version 5.1 Firewall

The Sidewinder™ application proxy firewall will be our primary gatekeeper for the GIAC Enterprises infrastructure. Leveraging the firewalls http and Web proxy capabilities and by placing the e-commerce (EC_GIAC Network) network on it's own Burb greatly enhances our ability to control access, monitor, and mitigate the risks associated with hosting a website. We will also utilize the VPN feature of the Sidewinder firewall to provide secure remote access to the private (PC_GIAC Network) network via the Internet. The Sidewinder was chosen for its inherently strong security posture and record. This was a very important consideration with the protection of sensitive networks such as the EC_GIAC Network and the PC_GIAC Network. Other implementation consideration factors are split DNS, mail filtering, web traffic filtering and Network Address Translation.

Intel® NetStructureÔ 3130 VPN Gateway Version 6.8.1

The Intel® 3130 will provide supplier and international business partner access to the supplier/partner (SP_GIAC Network) network via a VPN service. The Intel 3130 was chosen because it offers the option to use standard IPSEC and L2TP protocols as well as the proprietary Intel Shiva® Smart Tunnel (SST). This should enable more manageable interoperations with future business partners and/or suppliers. Utilizing SST will allow for an easier establishment and maintenance of separate tunnel groups of which we can set security associations, policy, and network access controls for each as required. The multiple VPN type selections, policy creation capabilities, and the detail in which they can be created is key in the 3130's selection, especially due to the cryptographic restrictions in dealing with international partners. The appliance also features an ICSA-certified circuit level firewall to compliment VPN controls and access. The 3130 will allow you to designate tunnel endpoints either before or after the firewall. This allows for further enhanced policy by services allowed or disallowed via the tunnel to the SP_GIAC Network

FreeBSD Version 4.3 IPFW Firewall

The FreeBSD IPFW stateful packet filtering firewall will enhance the protection for our private (PC_GIAC Network) corporate network. It will also help to insure proper access control into the PC_GIAC Network as well as exercising a layered security approach. Although through the use of VPN security associations we can limit access supplier and partner access to the SP_GIAC Network, the placement of the IPFW Firewall will further enforce that policy as well as enforcing policy on access and services to the SP_GIAC Network from the PC_GIAC Network. The IPFW is a very cost effective solution as well as being easily managed in this particular architecture.

Assignment Two: Security Policy for GIAC Enterprises

Introduction

The creation and implementation of an effective perimeter protection security policy require that guidelines be established before the creation process. Along with these guidelines there is the need that other system security policies, plans, and practices are in place. These along with the perimeter protection security policy; become the GIAC Enterprises Information Systems Security Policy. This approach improves the overall security posture of an enterprise and implements a layered security approach. Most of these are not covered in depth as are they not within the scope of perimeter protection as it pertains to this particular architecture, but they would include such items as service or resource hardening; such as web, DNS, and mail servers, internal host security, local user and group policies, local security practices, virus prevention, along with configuration management, and operations security as a whole.

The following guidelines (NSA, p.41) and checks will be taken into accordance in the creation of the GIAC Enterprises Perimeter Protection Security Policy. The foundation of these definition guidelines are taken from the above noted reference and pertain to a particular device, however these guidelines can be applicable in developing each of the individual perimeter device's security policy.

Physical Security

- Designates who is authorized to install, de-install, and move a device.
- Designates who is authorized to perform hardware maintenance and to change the physical configuration of a device.
- Designates who is authorized to make physical connections to a device.
- Defines controls on placement and use of console and other direct access port connections.
- Defines recovery procedures for the event of physical damage to a perimeter device, or evidence of tampering with a device.

Static Configuration Security

- Designates who is authorized to log in directly to the device via the console or other direct access port connections.
- Designates who is authorized to assume administrative privileges on the device.
- Defines procedures and practices for making changes to the device static configuration (e.g. log book, change recording, review procedures)
- Defines the password policy for user/login passwords, and for administrative or privilege passwords.
- Designates who is authorized to log in to the device remotely.
- Designates protocols, procedures, and networks permitted for logging in to the device remotely.
- Defines the recovery procedures, or identifies individual responsible for recovery, in the case of compromise of the device's static configuration.
- Defines the audit log policy for the device, including outlining log management practices and procedures.
- Designates procedures and limits on use of automated remote management and monitoring facilities (e.g. SNMP)

- Outlines response procedures or guidelines for detection of an attack against the device.
- Defines the key management policy for long-term cryptographic keys (if any).

Dynamic Configuration Security

- Identifies the dynamic configuration services permitted on a device, and the networks permitted to access those services.
- Identifies the specific protocols to be used, and the security features to be employed on each if any.
- Designates mechanisms and policies for setting or automating maintenance of the device's clock (e.g. manual setting, NTP)
- Identifies key agreement and cryptographic algorithms authorized for use in establishing VPN tunnels with other networks (if any).

Network Service Security

- Enumerates protocols, ports, and services to be permitted or filtered by the device, OR identifies procedures and authorities for authorizing them.
- Defines response procedures, authorities, and objectives for the event of detection of attack against the network.
- Only network services that have an operational or business requirement should be allowed, unnecessary services should not be active or filtered.
- Only operational or business requirements to traverse any network boundary should be allowed.

Scope

The GIAC Enterprises security policy for each of its perimeter protection components shall be detailed in this section. The policy shall explain the rules and access controls that have been implemented with each device to create the GIAC Enterprises Perimeter Protection Security Policy.

In this instance, the fictitious GIAC Enterprises domain has been assigned Public Class C addresses 212.212.5.129-254/25. *(This selection was done completely at random and is not intended to represent an actual company or organization. The selection was for the sole purpose of this exercise.)* Public addresses 129-131 will be accessible from the Internet and shall provide access points to PC_GIAC (10.2.0.0/16), SP_GIAC (10.3.0.0/16), and the EC_GIAC (10.1.0.0/16) Networks.

GIAC Enterprises Border Router Policy

The GIAC Enterprises Cisco® 4000 security policy will be formulated using the previously stated guidelines as well as satisfying GIAC Enterprises business requirements. Further guidance will come from other sources such as the SANS Firewalls, Perimeter Protection, and VPNS [Brenton] course curriculum and the National Security Agency's Router Security Configuration Guide [NSA]. The policy will focus on utilizing the router's security strengths and to compliment our GIAC Firewall Security Policy. (Brenton, p.11) A router's strengths are:

- Anti-spoofing
- Block private addressing

- Control ICMP traffic
- Block source routing

Along with these capabilities we shall facilitate access control measures on the router itself to prevent it from becoming compromised and used maliciously against itself or other networks.

Physical Security

- The GIAC Router will be located in a controlled access area. Only authorized personnel will be granted access.
- Any physical access to the router will be by authorized GIAC Enterprises staff and/or vendor maintenance personnel only. Vendor maintenance personnel must have authorized GIAC personnel escort.
- Any maintenance or physical configuration change to the router will be by authorized GIAC Enterprises and/or vendor maintenance personnel only. Vendor maintenance personnel must have authorized GIAC personnel escort.
- Router console and all other direct access port connections will be located in same controlled access area as the router.

Static Configuration Security

- Only personnel designated by the GIAC Enterprises Information Systems Security Officer (ISSO) are authorized to login to the router. Authorized personnel with administrator privileges are designated by the ISSO. The router login banner will denote this.
    - giacent# config t
    - giacent(config) # banner login 0 #
      THIS GIAC ENTERPRISE SYSTEM IS FOR AUTHORIZED GIAC USE ONLY. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION.
      #
    - giacent(config) # end
- The GIAC Enterprises password policy will be applied for all logins. The password must be at least 8 characters in length, have at least on special character and one capital letter. Passwords will be protected and encrypted locally.
    - giacent# config t
    - *!!configures username for unprivileged login!!*
    - giacent(config)# username giacadmin privilege 1 password $is2GIAC
    - *!!generates an MD5 hash of the enable mode password!!*
    - giacent(config)# enable secret 5 Time2GIAC
    - *!!Insures only the enable mode secret password is in the config!!*
    - giacent(config)# no enable password
    - *!!Prevents "shoulder surfing" of passwords!!*
    - giacent(config)# service password-encryption
    - giacent(config) # end

- Router login will be required and allowed at the local console ONLY, remote access or auxiliary access will not be allowed. Inactivity timeouts will be enforced on the console
    - *!! These commands secure the console and enforce inactivity timeout!!*
    - giacent# config t
    - giacent(config) # line con 0
    - giacent(config-line) # transport input none
    - giacent(config-line) # login local
    - giacent(config-line) # exec-timeout 5 0
    - giacent(config-line) # end
    - *!! These commands secure the routers virtual terminals!!*
    - giacent# config t
    - giacent(config) # no access-list 50
    - giacent(config) # access-list 50 deny any log
    - giacent(config) # line vty 0 4
    - giacent(config-line) # access-class 50 in
    - giacent(config-line) # transport input none
    - giacent(config-line) # login local
    - giacent(config-line) # exec-timeout 0 1
    - giacent(config-line) # no exec
    - giacent(config) # end
    - *!! These commands secure the Aux input !!*
    - giacent# config t
    - giacent(config) # line aux 0
    - giacent(config-line) # transport input none
    - giacent(config-line) # login local
    - giacent(config-line) # exec-timeout 0 1
    - giacent(config-line) # no exec
    - giacent(config-line) # end

- Remote monitoring and remote management tools will not be allowed
    - giacent# config t
    - *!! Disables the web remote management interface!!*
    - giacent(config) # no ip http server
    - giacent(config) # end
    - *!! Removes any prior SNMP configurations and Disables Simple Network Management Protocol (SNMP)!!* (NSA, p67)
    - *!!Remove old communities if exist!!*
    - giacent(config) # no snmp community public RO
    - giacent(config) # no snmp community admin RW
    - *!!Establish a prohibitive access list!!*
    - giacent(config) # no access-list 70
    - giacent(config) # access-list 70 deny any
    - *!!Make snmp read only and subject to access!!*
    - giacent(config) # snmp community 1a2b3c4d7890 ro 70
    - *!!Disable traps and shutdown features!!*

    - giacent(config) # no snmp enable traps
    - giacent(config) # no snmp system-shutdown
    - giacent(config) # no snmp trap-auth
    - *!!Disable SNMP service!!*
    - giacent(config) # no snmp-server
    - giacent(config) # end
- All logins to the router will be logged and documented in the local router logbook as to "who, what, and why" of the login.
- Remote logging to the protected network will be utilized to provide audit and alert functions.
    - *!!These commands will establish our logging to a central protected syslogger!!*
    - giacent # config t
    - giacent(config) # logging trap information
    - giacent(config) # logging 212.212.5.129 *!!SidewinderÔ Firewall external IP for proxy!!*
    - giacent(config) # logging facility local6
    - giacent(config) # logging source-interface eth0
    - giacent(config) # end
- The GIAC Enterprises Information Systems Security Officer will have the ultimate responsibility of insuring that daily audit activities are reviewed.
- All configuration changes will be reviewed by the ISSO and logged as implemented.

Dynamic Configuration Security

- No dynamic configuration will be allowed
    - *!!These lines enable auto startup configuration from local memory only!!*
    - giacent# config t
    - giacent(config) # no boot network
    - giacent(config) # no service config
    - *!!These lines disable Network Time Protocol (NTP) on all interfaces!!*
    - giacent(config) # int s0
    - giacent(config-if) # no ntp enable
    - giacent(config-if) # exit
    - giacent(config) # int s1
    - giacent(config-if) # no ntp enable
    - giacent(config-if) # exit
    - giacent(config) # int eth 0
    - giacent(config-if) # no ntp enable
    - giacent(config-if) # end

Network Services Security

- Non-operationally required services should not be active and required services should be implemented with access restriction
    - *!!The tcp/udp small servers offer frequently exploitable ports!!*
    - giacent# config t

- giacent(config) # no service tcp-small servers
- giacent(config) # no service udp-small servers
- *!!Unnecessary layer 2 communications between Cisco® devices!!*
- giacent(config) # no cdp run
- *!!Finger service enables information leaks such as user names!!*
- giacent(config) # no service finger
- giacent(config) # no ip finger
- *!! bootp can provide information leaks!!*
- giacent(config) # no ip bootp server
- *!!source routing can be used in a variety of attacks!!*
- giacent(config) # no ip source-route
- *!!rejects illegal address packets!!*
- giacent(config) # no ip subnet-zero
- *!! disables name server queries, unnecessary service!!*
- giacent(config) # no ip name-server
- *!!Prevents routing of unknown destination IP packets!!*
- giacent(config) # no ip classless

Interface Specific, Business (Desired) Services, and Access Control Lists

- The following IOS commands are used to implement the desired services on the associated interfaces. Filters will be imposed on the router's interfaces to inhibit traffic other than valid ingress or egress traffic to GIAC Enterprises networks. The filters imposed will all be via Cisco® IOS Extended Access Lists (access list numbers 100-199). Extended Access Lists can permit or deny packets based on protocol, source or destination ip addresses, source or destination TCP/UDP ports, or ICMP or IGMP message types. Standard Access Lists (list number 1-99) allow only source IP address filtering.
  - *!!We don't want Proxy-ARP, ICMP Unreachable, ICMP Directs, Redirects, or ICMP Mask Replies on ANY interface to prevent network mapping and SMURF attacks !!*
  - giacent # config t
  - giacent(config) # interface s0
  - giacent(config-if) # no ip proxy-arp
  - giacent(config-if) # no ip unreachable
  - giacent(config-if) # no ip redirect
  - giacent(config-if) # no ip mask-reply
  - giacent(config-if) # no ip directed-broadcast
  - giacent(config-if) # exit
  - giacent(config) # interface s1
  - giacent(config-if) # no ip proxy-arp
  - giacent(config-if) # no ip unreachable
  - giacent(config-if) # no ip redirect
  - giacent(config-if) # no ip directed-broadcast
  - giacent(config-if) # no ip mask-reply
  - *!!Serial Interface 1 is unused so it will be shutdown!!*
  - giacent(config-if) # shutdown

    - giacent(config-if) # exit
    - giacent(config) # interface eth 0
    - giacent(config-if) # no ip proxy-arp
    - giacent(config-if) # no ip unreachable
    - giacent(config-if) # no ip redirect
    - giacent(config-if) # no ip directed-broadcast
    - giacent(config-if) # no ip mask-reply
    - giacent(config-if) # exit
- Extended Access Control List Entries
    - ***!! For eth 0, outbound from GIAC ENT to ISP!!***
    - giacent(config) # no access-list 100
    - *!!Permit all traffic from the GIAC Enterprises Networks!!*
    - giacent(config) # access-list 100 permit ip 212.212.5.128 0.0.0.127 any
    - *!! Deny all other traffic and log!!*
    - giacent(config) # access-list 100 deny ip any any log
    - *!! Implement the Extended Access List on Interface Ethernet 0!!*
    - giacent(config) # interface eth 0
    - giacent(config-if) # ip access-group 100 in
    - giacent(config-if)# exit
    - ***!! For serial 0 interface, inbound from ISP to GIAC Ent!!***
    - giacent(config) # no access-list 101
    - *!! Drops and logs traffic spoofed with our public address!!*
    - giacent(config) # access-list 101 deny ip 212.212.5.128 0.0.0.127 any log
    - *!! Drops and logs traffic spoofed local loopback and illegal address!!*
    - giacent(config) # access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
    - giacent(config) # access-list 101 deny ip 0.0.0.0 255.255.255.255 any log
    - *!! Drops and logs traffic with any spoofed private addresses!!*
    - giacent(config) # access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
    - giacent(config) # access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
    - giacent(config) # access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
    - giacent(config) # access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
    - *!! Drops and logs any inbound ICMP echo PING packets!!*
    - giacent(config) # access-list 101 deny icmp any any echo log
    - *!! Drops and logs any inbound ICMP redirect packets!!*
    - giacent(config) # access-list 101 deny icmp any 212.212.5.128 0.0.0.127 redirect log
    - *!!Permits established GIAC traffic!!*
    - giacent(config) # access-list 101 permit tcp any any established
    - *!! Allows web traffic!!*
    - giacent(config) # access-list 101 permit tcp any 212.212.5.128 0.0.0.127 eq 80
    - *!!Allows SSL traffic!!*
    - giacent(config) # access-list 101 permit tcp any 212.212.5.128 0.0.0.127 eq 443
    - *!!Allows IKE traffic!!*

- giacent(config) # access-list 101 permit udp any 212.212.5.128 0.0.0.127 eq 500
- *!!Allows ESP VPN traffic!!*
- giacent(config) # access-list 101 permit tcp any 212.212.5.128 0.0.0.127 eq 50
- *!!Allows SMTP traffic!!*
- giacent(config) # access-list 101 permit tcp any 212.212.5.128 0.0.0.127 eq 25
- *!!Allows Shiva Secure Tunnel (VPN) traffic!!*
- giacent(config) # access-list 101 permit udp any 212.212.5.128 0.0.0.127 eq 2233
- *!!Allows DNS traffic!!*
- giacent(config) # access-list 101 permit udp any 212.212.5.128 0.0.0.127 eq domain
- *!!All other traffic is denied and logged!!*
- giacent(config) # access-list 101 deny ip any any log
- *!!Implement the extended access-list on Serial Interface 0!!*
- giacent(config) # interface s0
- giacent(config-if) # ip access-group 101 in
- giacent(config-if) # exit

GIAC Enterprises Primary Firewall Policy

As stated previously the Secure Computing Corporation's Sidewinder™ Version 5.1 Firewall is the primary gatekeeper for the GIAC Enterprises infrastructure. The Sidewinder is defined as a network security gateway. Sidewinder provides a high level of security by using SecureOS™, a highly secure UNIX operating system that employs Secure Computing's patented Type Enforcement security technology. Type Enforcement places tight control over how data files are shared among the processes running on a system. It does this buy using application specific domains, controlling the domains that a process can access, controlling the files a process can access, controlling users access to domains using administrator roles, and controlling system calls. Type Enforcement and SecureOS removes the inherit risks of layering a firewall application on top of a discrete commercial operating system. (Secure, p1-2 through 1-7) The Sidewinder also employs Strikeback™ technology, which is a configurable action, or actions that the Sidewinder performs when an alarm occurs. Sidewinder includes Windows NT as well as UNIX interface options. The interface, known as "Cobra," presents a uniform look and feel on both UNIX and NT platforms. Both versions of Cobra are built from the same code base, and offer the exact same functionality and the same Explorer-style tree structure for all services.

The primary firewalls will regulate all inbound/outbound Internet (burb 2) traffic into the GIAC Enterprises PC_GIAC (burb 1) and EC_GIAC (burb 3) Networks as well as traffic in between the two networks.

GIAC Primary Firewall Burb Reference Table:

PC_GIAC	Internet	EC_GIAC
Burb 1	Burb 2	Burb 3
Internal	External	DMZ
Index 1	Index 2	Index 3

Physical Security

- The GIAC primary firewall will be located in a controlled access area. Only authorized personnel will be granted access.
- Any physical access to the router will be by authorized GIAC Enterprises staff and/or vendor maintenance personnel only. Vendor maintenance personnel must have authorized GIAC personnel escort.
- Any maintenance or physical configuration change to the firewall will be by authorized GIAC Enterprises and/or vendor maintenance personnel only. Vendor maintenance personnel must have authorized GIAC personnel escort.
- The Firewall system console will be located in same controlled access area as the firewall.

Static Configuration Security

- Only personnel designated by the GIAC Enterprises Information Systems Security Officer (ISSO) are authorized to login to the firewall. The firewall will display a motd (Message Of The Day) banner referencing this.
    - giacfw# cat /etc/motd THIS GIAC ENTERPRISE SYSTEM IS FOR AUTHORIZED GIAC USE ONLY. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION.
- Authorized personnel with administrator privileges are designated by the ISSO.
- The GIAC Enterprises password policy will be applied for all logins. The password must be at least 8 characters in length, have at least on special character and one capital letter.
- RMON or SNMP will not be allowed.
- Authorized personnel will be allowed administrative access via Secure Cobra Management channels or local system console ONLY. Remote administration other than the local system console is restricted to the internal burb ONLY! Access control lists (ACL) will be established and the Cobra Management will be configured accordingly. The following two figures reflect this.

  (NOTE: This ACL rule should be placed near the bottom of the ACL with the more commonly used ACLs placed at the top as the list is processed from the top to the bottom)

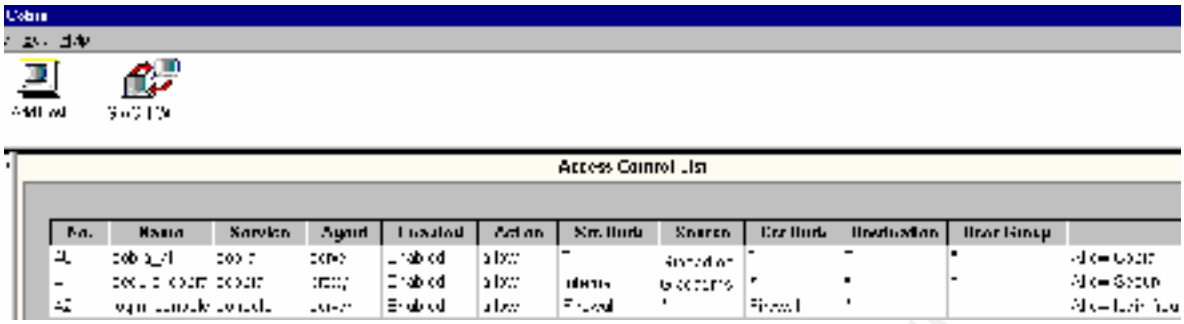


Figure 2. ACL for Cobra and Secure Cobra

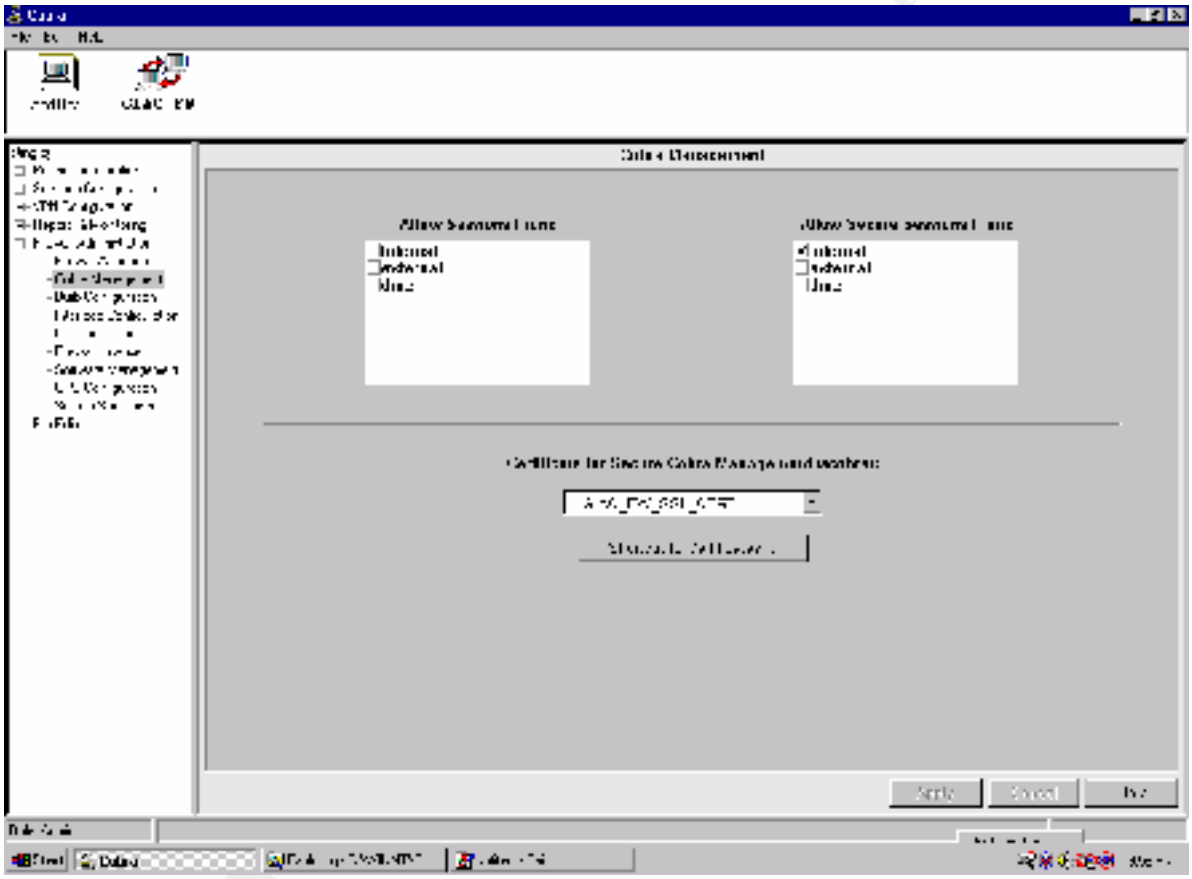


Figure 3. Cobra Management Configuration

- The GIAC Enterprises ISSO will review and approve all configuration changes.
- All logins to the firewall will be logged and in the local firewall audit files, a local file will be kept as to "who, what, and why" of the login.
- Audit logs and reports will be generated daily and emailed to the ISSO and firewall administrators for review. The Sendmail a*liases* file will be edited as all reports default to the local root account.
    - Log in to the Sidewinder and type the following command to change to the admin role. The system will return a UNIX prompt.
    - **/usr/bin/srole admin**

    - Open the /etc/aliases file using a text editor and edit it as necessary to redirect all of roots mail to giac_admins@giacent.com
    - Locate the root line in the file and edit it to look like this: **root: giac_admins@giacent.com**
    - rebuild the alias database: **/usr/bin/newaliases**
    - The following message will be displayed: "Rebuilding the internal mail aliases."
- Alarm events will be emailed to the ISSO and firewall administrators. (giacadmins) Attack and UPS notifications will be sent via pager as well. Each alarm event has an associated threshold, a period, and a response.
    - **Threshold**--The threshold specifies the number of times an event must occur in a specified period before an alarm will be triggered.
    - **Period**--The period specifies the amount of time during which the number of events specified by the Threshold must occur before an alarm is triggered.
    - **Response**--The response indicates one or more of the four possible responses for the alarm event. The responses are email, pager, Strikeback, and SNMP trap.
    - Attack alarms will also result in Strikeback response. The default Strikeback configuration will execute a **"dig"** command against the offending source. The dig (Domain Information Groper) command provides information on an IP address via Domain Name Service queries. The results will be emailed to the **giacadmins** alias created above. See Figures 4 & 5.

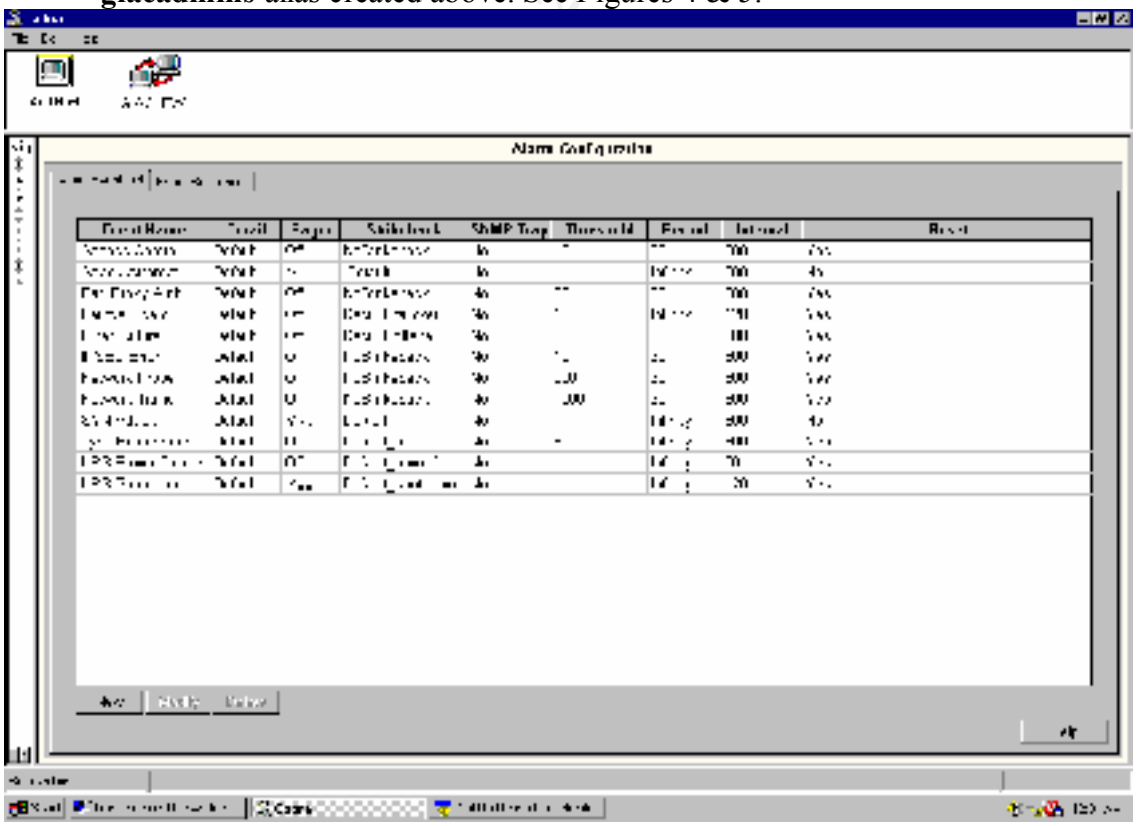
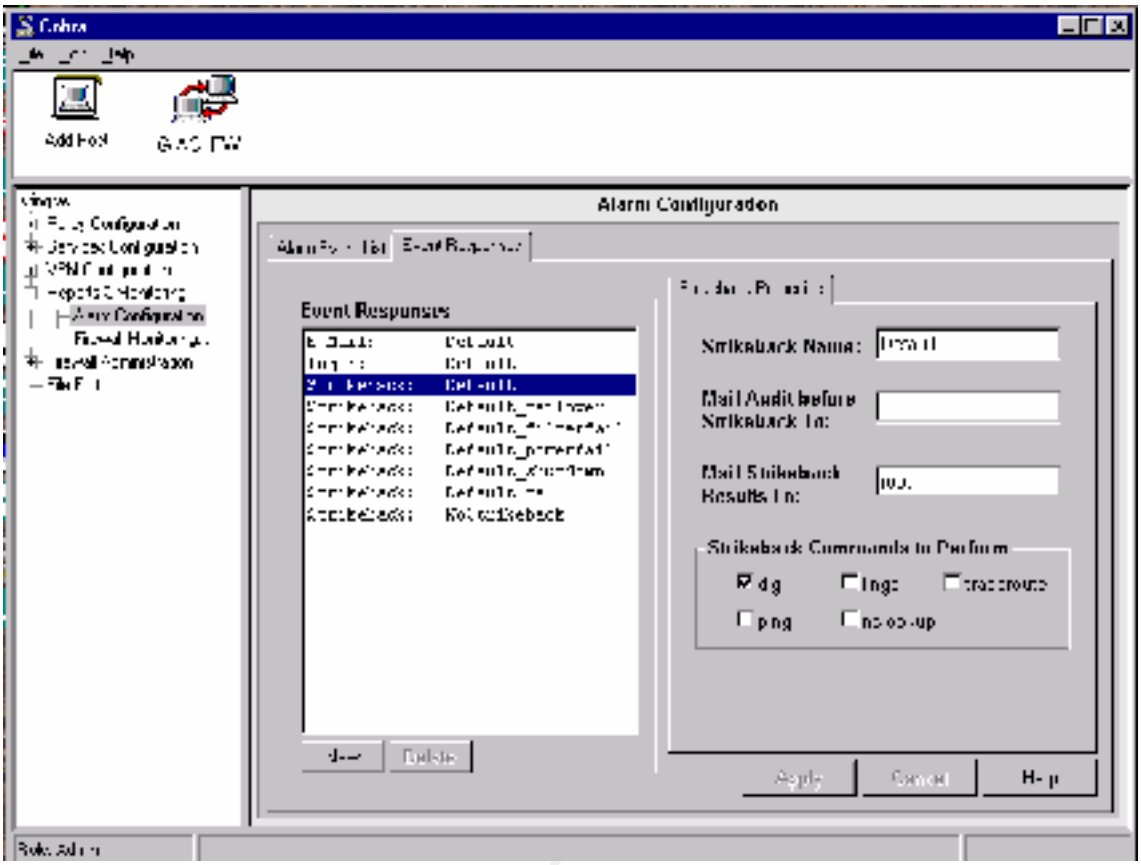


Figure 4. Alarm Configuration



Figures 5. Alarm Configuration Event Response

Dynamic Configuration Security

- System clock time will be updated via an NTP peer from the internal Burb.
  - Login to the firewall and srole to the admin domain: **/usr/bin/srole admin**
  - Disable the current clock correction utility. **cf server disable fixclock**
  - Create the default NTP configuration file. **cf ntp config burb=internal**
  - Configure the Select the machine(s) from which the Sidewinder will receive time. **cf ntp add server burb=internal ip=10.2.x.x** (internal NTP Server)
  - Enable NTP in the desired Burb. **cf server enable ntp burb=internal**
- No other dynamic configuration will occur for the GIAC Enterprises primary firewall.

Network Services Security

Only business required network services are allowed to transverse the firewall. Each network service's use, control, and integrity will be insured by the firewall. The GIAC Enterprises firewall will have a large role in handling the core primary services of Domain Name Service, Simple Mail Transport Protocol, and web access for GIAC Enterprises. Each of the required services will be addressed in this section.

- The GIAC Enterprises primary firewall external burb will be configured so that all unreachable services are filtered and that ICMP redirects, timestamps, and echoes are

not honored. This helps to insure obscurity of the firewall (e.g. timestamps) and any information that may be obtained via ICMP or other malicious intent stimuli. See Figure 6.

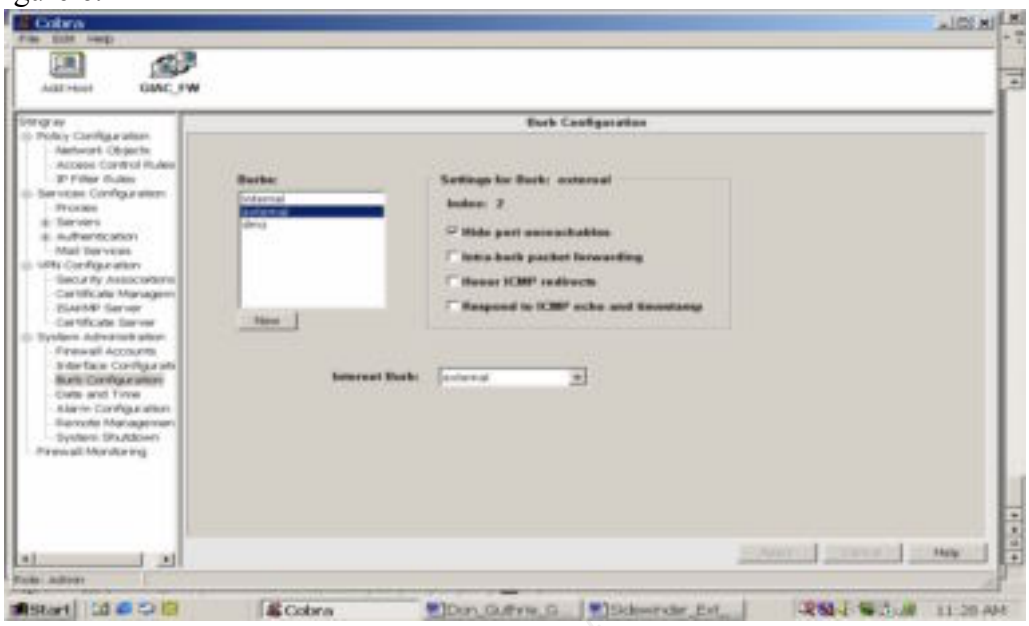


Figure 6 Burb Configuration

Sidewinder Email (Sendmail)

In order to set an effective policy, it is important to have an understanding of Sendmail on the Sidewinder firewall. The firewall actually runs three separate Sendmail servers that all have different purposes. (*Secure*, 8-1 thru 2)

- *Local*- The local server handles mail that is sent from the firewall itself
- *Internal*- The internal server runs in the trusted internal Burb and receives mail from one of three sources:
  1. A host on the internal network
  2. The mfil_queue_mail program transferring mail from the local Sendmail server
  3. The mfil_queue_mail program transferring mail from the external Sendmail server

The internal server delivers mail to one of three places:

1. If the message is for a user local on the Sidewinder it delivers the message to the user's mailbox using the mail.local program.
2. If the message is for a user on the internal network, it connects to the mail host on the internal network and delivers the mail there.
3. If the message isn't for either of the above, it assumes the message is for an Internet user and uses mfil_queue_mail to transfer the message to the Internet.

- *Internet*- The Internet server runs in the *mta#2* domain and this Sendmail daemon receives mail from one of two sources:
  1. A host on the external network
  2. The mfil_queue_mail program transferring mail from the internal Sendmail server

The external server delivers mail to one of two places:

1. If the message is for a user on the Internet, it connects to a host on the Internet and delivers the mail there.

2. If the message is for a user local to the Sidewinder (such as an administrator) *or* for a user on the internal network, it delivers the mail to the internal Sendmail server using the mfil_queue_mail program.

Type Enforcement also restricts Sendmail so that security flaws cannot be exploited. For example, users cannot execute shell scripts or other executables through Sendmail on the Sidewinder, as they could do on a standard UNIX system.

Sendmail (SMTP) Service Policy

- Authorized relay domains will be configured in the access table on the internal (/etc/access.mta1) and external (/etc/access.mta2) SMTP servers to accept mail only for **giacent.com**. An ACL will also be established to allow only relaying from the internal mail server to the internal burb. Figures 7-8 reflect this configuration.

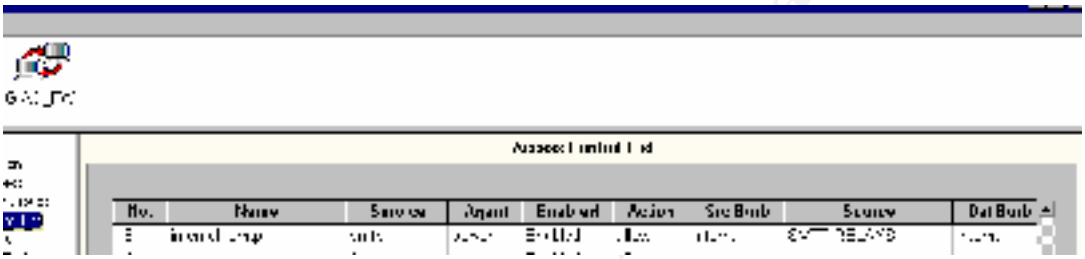


Figure 7. SMTP ACL

NOTE: Considerations should be given in assigning this ACL a lower number (toward the top of the list), as the rule match should come early in processing due to SMTP traffic volume.

NOTE: The source and destination burbs are both Internal on this ACL due to the operations described above.

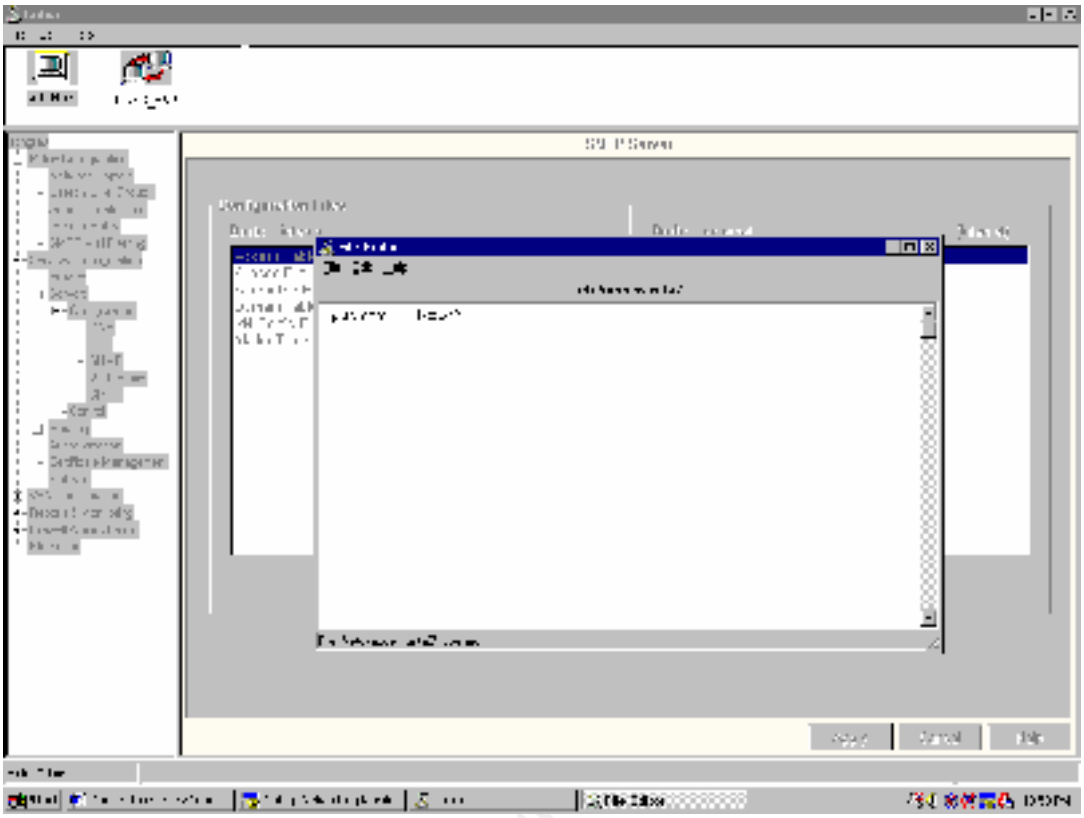


Figure 8. Authorized Relay Domains /etc/access.mta$

Sidewinder Web Proxies

Likewise as with Sendmail, the Sidewinder HTTP and Web Proxy need to be understood before policy can be established.

- The Sidewinder Web Proxy is a Squid based proxy that supports content filtering, Java applet filtering, caching, and user authentication.
- The HTTP Proxy is a transparent proxy that offers URL header filtering.

Web Access (HTTP and SSL) Policy

- The GIAC Firewall Web Proxy will regulate all outbound established http (port 80) and https (port 443 for SSL) traffic from the PC_GIAC Network.
- Only authorized users will have access via the Web Proxy to EC_GIAC and/or the Internet. See Figure 9.

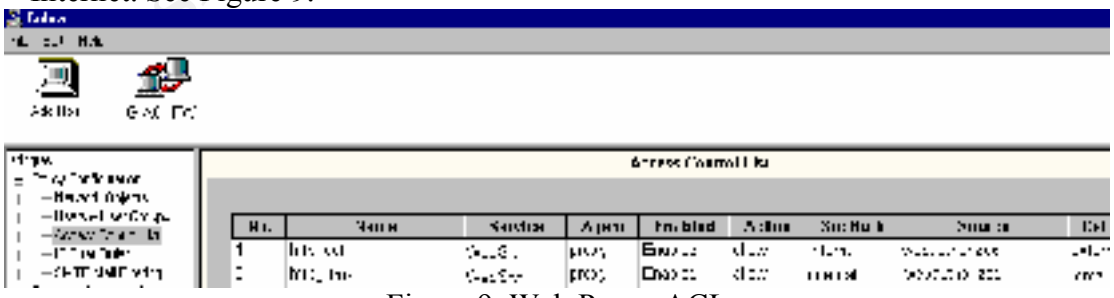


Figure 9. Web Proxy ACL

- EC_GIAC Network access from the Internet will be via http (port 80) and https (port 443 for SSL) proxies only.

- URL Header filtering will be applied with GET requests only being allowed
- Implementation considerations:
  - The http and https proxies must be created and enabled in the external burb
  - An public address alias IP (212.212.5.131) will be assigned to the external burb interface
  - A Network Object for the e-commerce web server must be created.
  - An ACL is created for both proxies with IP redirection to the private e-commerce server address. (10.1.0.2)
- In Figures 10-15 the http (port 80) proxy setup is shown.
- The same steps apply to the SSL (port 443) proxy and ACL with the exception of the external interface configuration of the alias IP is only required once.

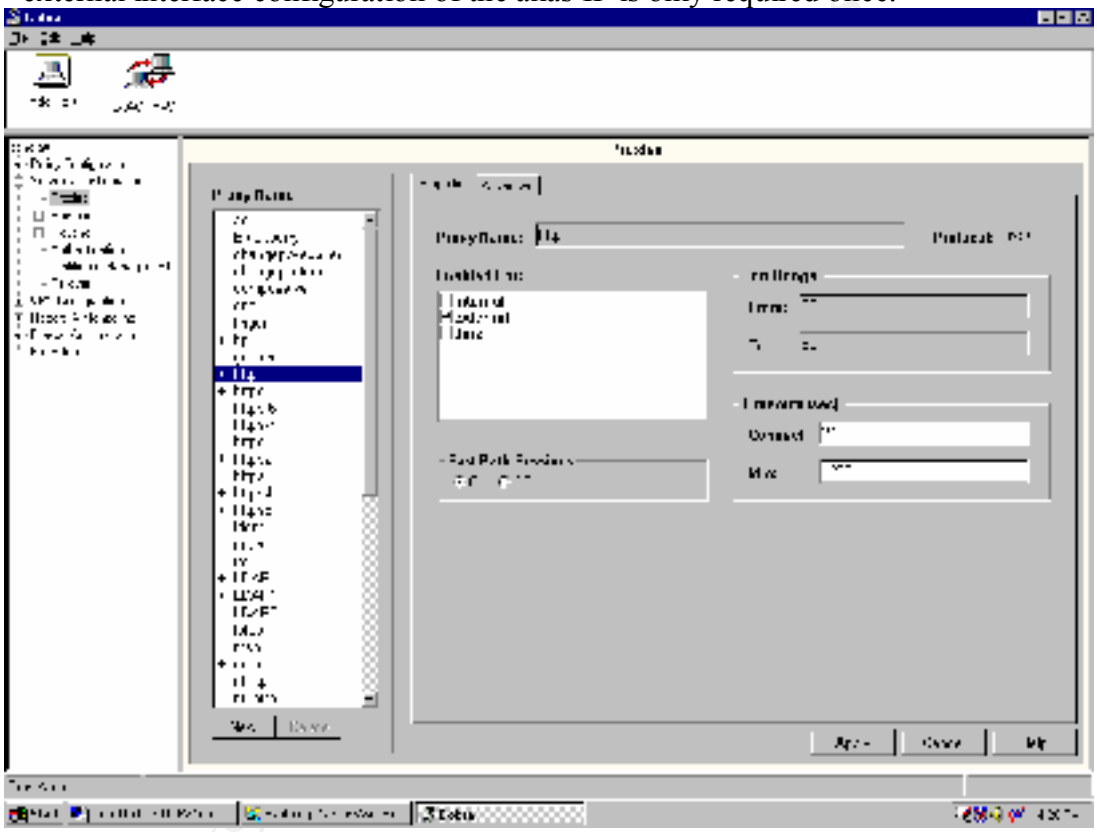


Figure 10.Proxy Creation

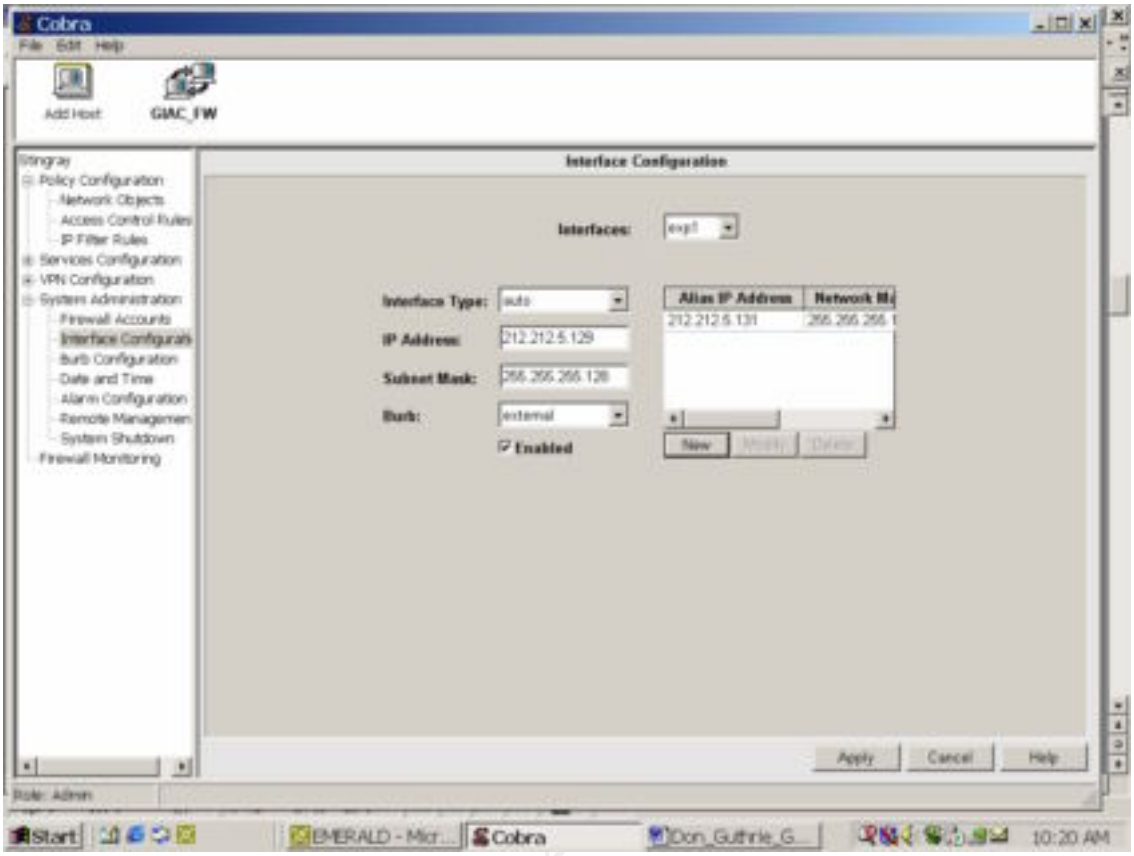


Figure 11. External Interface Configuration

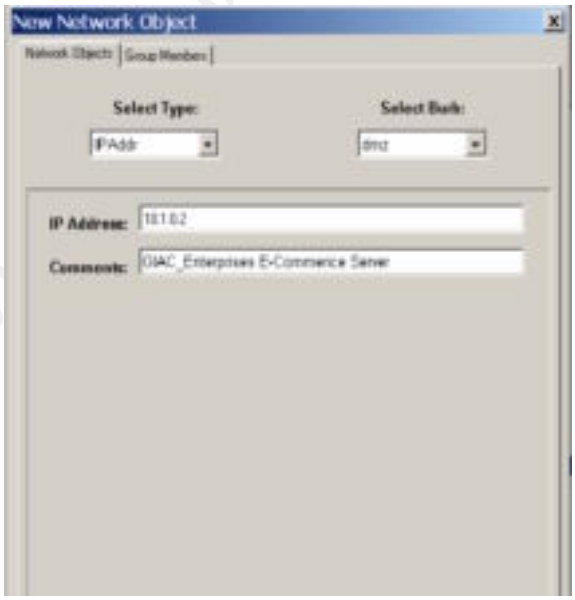


Figure 12. Network Object Creation

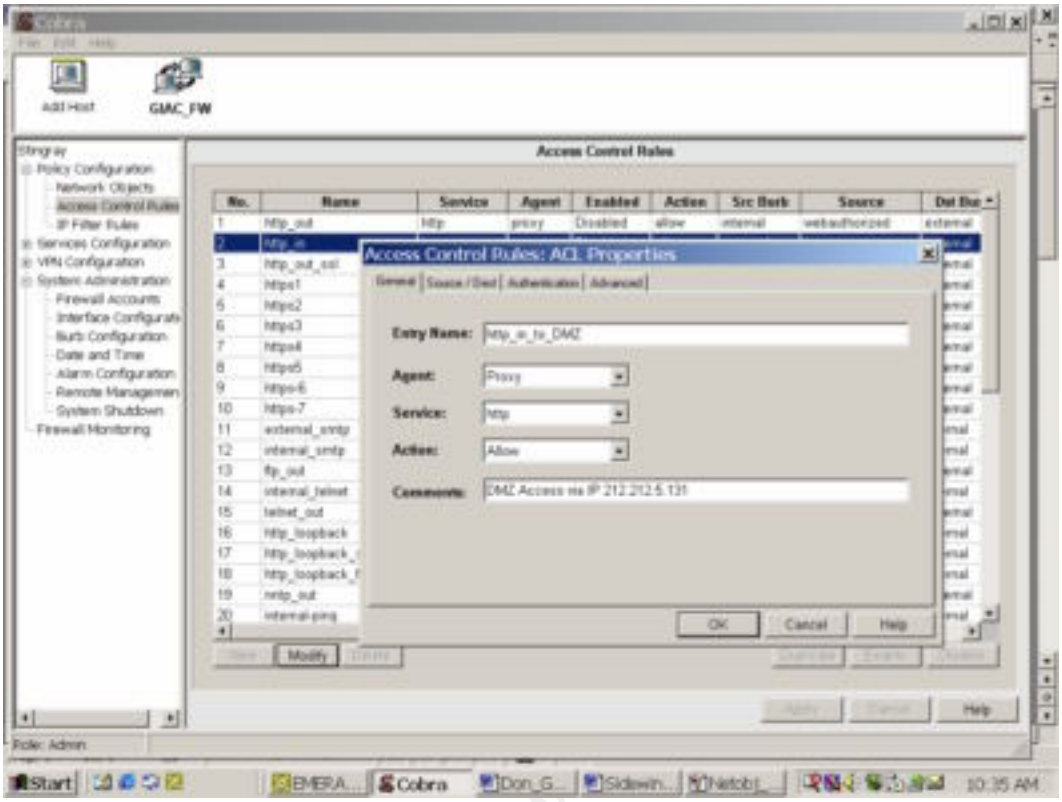


Figure 13. ACL http in Internet to EC_GIAC-General

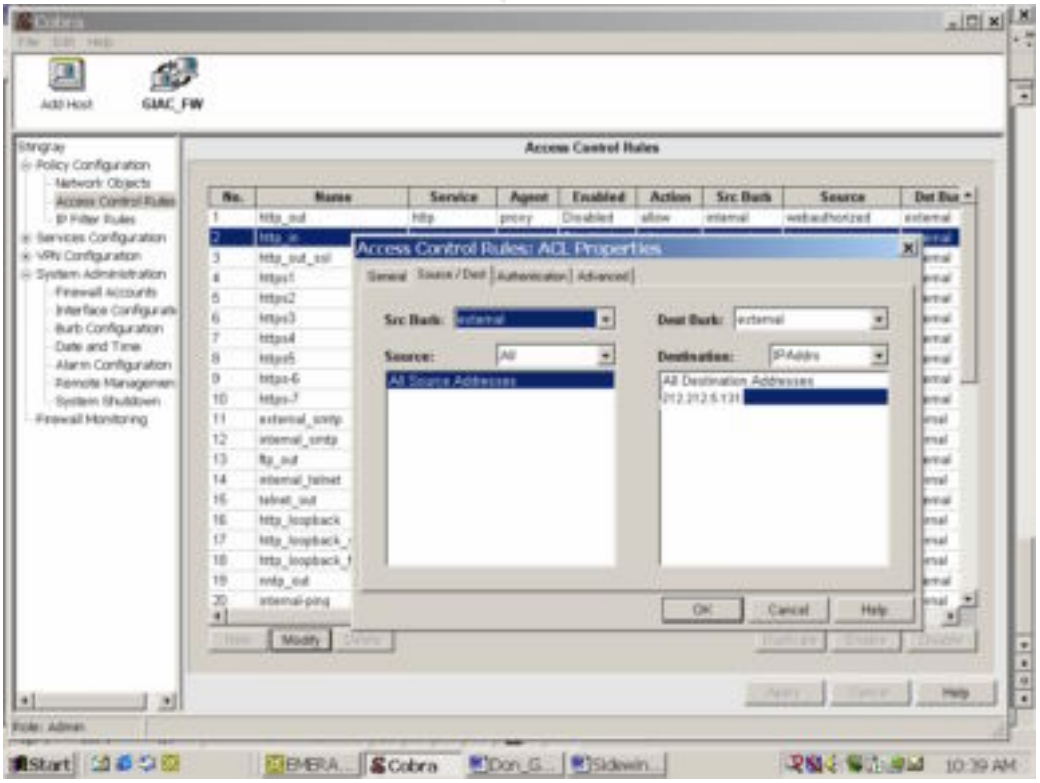


Figure 14. ACL http in Internet to EC_GIAC-Source/Destination
(Note: burb setting and destination of alias IP)

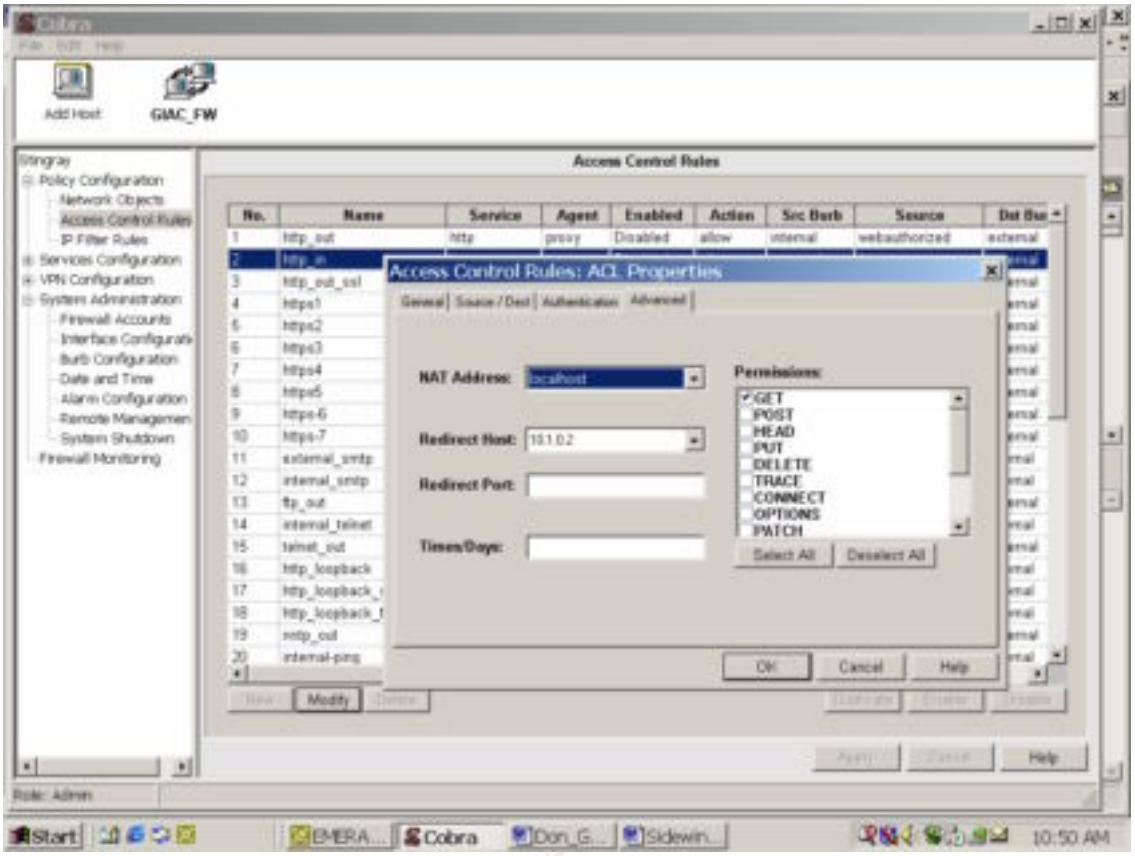


Figure 15. ACL http in Internet to EC_GIAC- Advanced
(Note: Permissions setting)

Domain Name Service

- The GIAC Enterprises primary firewall will run in a split DNS configuration. This is advantageous as it prevents the Internet community from knowing internal host names and IP addresses.
- The DNS server on the external burb will be authoritive for the giacen.com domain.
- The external DNS namedb database will contain only the required records for external business collaboration such as mail exchange (MX) records and public accessible server records.
- The external DNS cannot forward queries to the internal DNS, this is established automatically when running the **cf_dns** utility for split DNS.
- The DNS server on the internal burb will be master for the PC_GIAC Network and forward queries to the external DNS.

Remote Access VPN

The Sidewinder firewall supports four types of VPNs: (Secure, Chapter 11)
Manual key VPN: The most basic type, however, difficult to administer and maintain because of manual keying. It cannot be used for dynamic IP-assigned clients or gateways. Each VPN peer requires an individual VPN configuration.

Automatic key shared password VPN: Simplest to configure with the only authentication being the sharing of a password with the VPN peer. Cannot be used for dynamic IP-assigned clients or gateways. Each VPN peer requires its own Sidewinder VPN configuration.
Automatic key single certificate VPN: Uses certificates and public key cryptography to authenticate the remote peer. Each VPN peer's administrator must manually exchange public certificates. This type of VPN can be used with dynamic IP-assigned clients and gateways. Each peer certificate requires its own Sidewinder VPN configuration.
Automatic key certificate authority-based VPN: This type of VPN is ideally suited for roving client VPN peers (such as those using laptop computers). In this type of VPN, each VPN peer administrator must obtain a certificate signed by a certificate authority trusted by the other peer. This type of VPN can be used with dynamic IP-assigned clients and gateways. A single Sidewinder VPN configuration can be used to administer many VPN clients.

- The VPN type will be automatic key certificate authority-based. (This VPN's capability of supporting dynamic-IP clients; while offering scalability and lower administrative effort were the reasons this VPN type was chosen.)
- Certificates will be created, signed, and stored by a private GIAC Enterprises Certificate Authority (CA). See Figures 16-17 for CA configuration on the firewall.

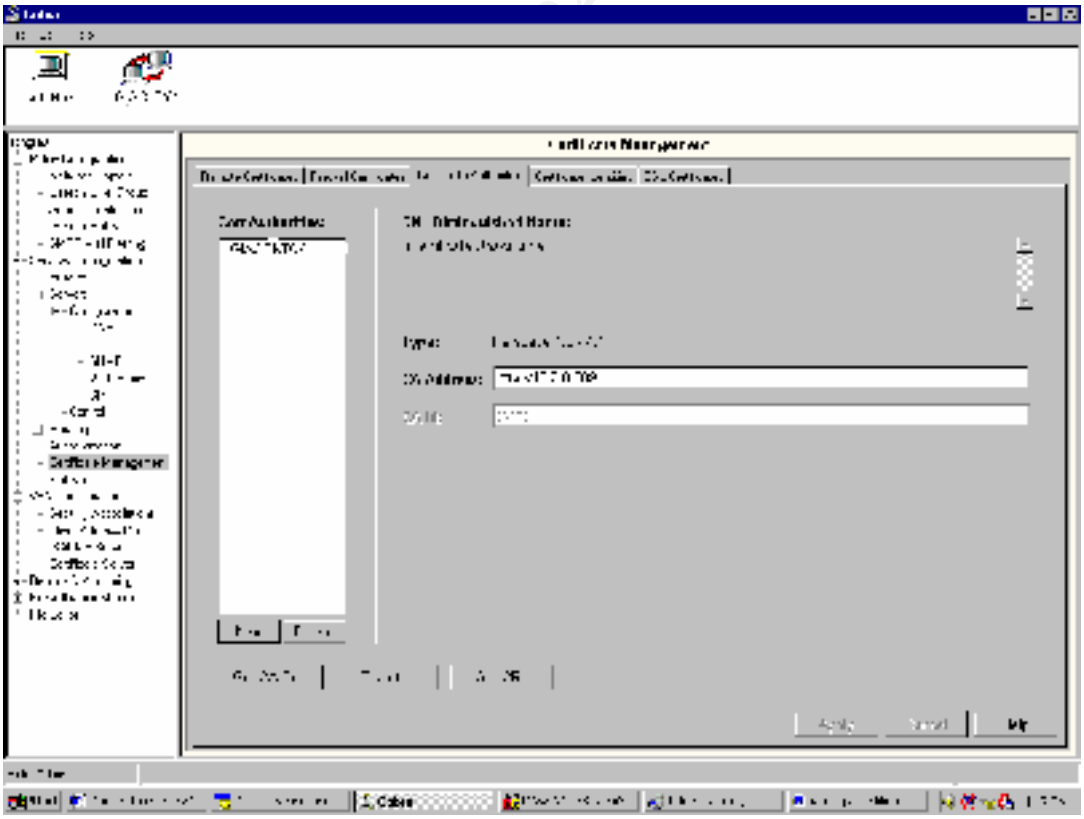


Figure 16. Certificate Authority Configuration

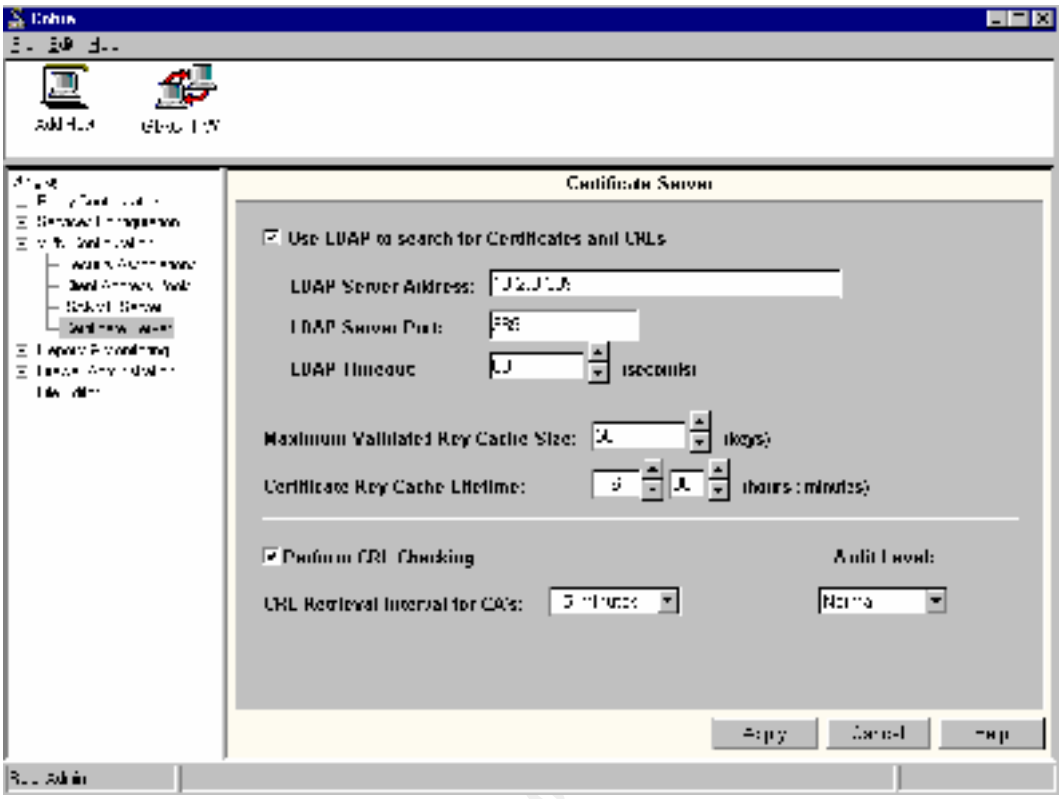


Figure 17. Certificate Server Configuration

- Remote Access to the PC_GIAC Network will only be available to authorized personnel that have business justifications for remote access.
- Individuals obtaining such access will first be briefed on their responsibilities as remote users and their role in the protection of GIAC Enterprises property and data.
- VPN Security Associations will be configured for access to the PC_GIAC Network only. (10.2.0.0)
- The VPN tunnel point will terminate at internal burb.
- The VPN will operate in tunnel mode (ESP) encapsulation to encrypt both data and source and destination IP information.
- Cryptographic algorithms used must be exportable due to international travel and export restrictions. This is due to the risk of accidental violation of export restrictions laws.
- ISAKMP and IPSEC forced re-keys will occur hourly, Perfect Forward Secrecy will also be employed. This is due to the use of weaker cryptographic algorithms.
- The ISAKMP Server will only be active on the external burb and utilize either certificates from local cache or the GIAC Enterprises LDAP server.
    - See Figures 18-22

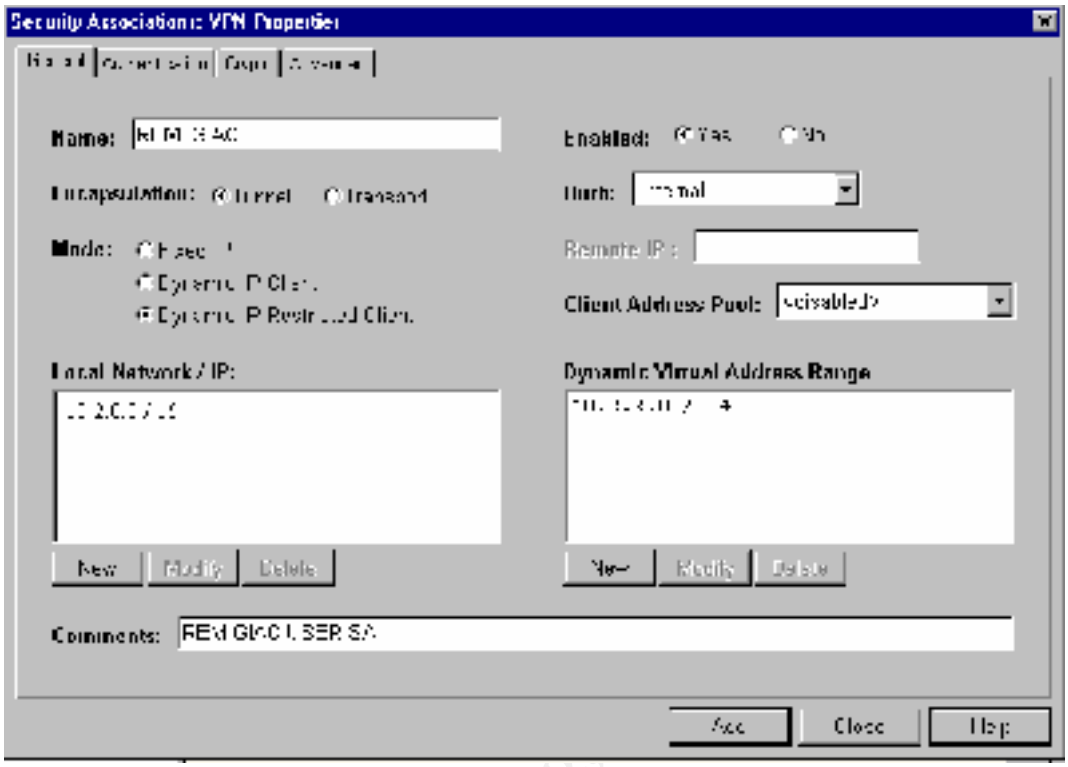


Figure 18. Security Association: General
(Note: Burb termination point and encapsulation mode)

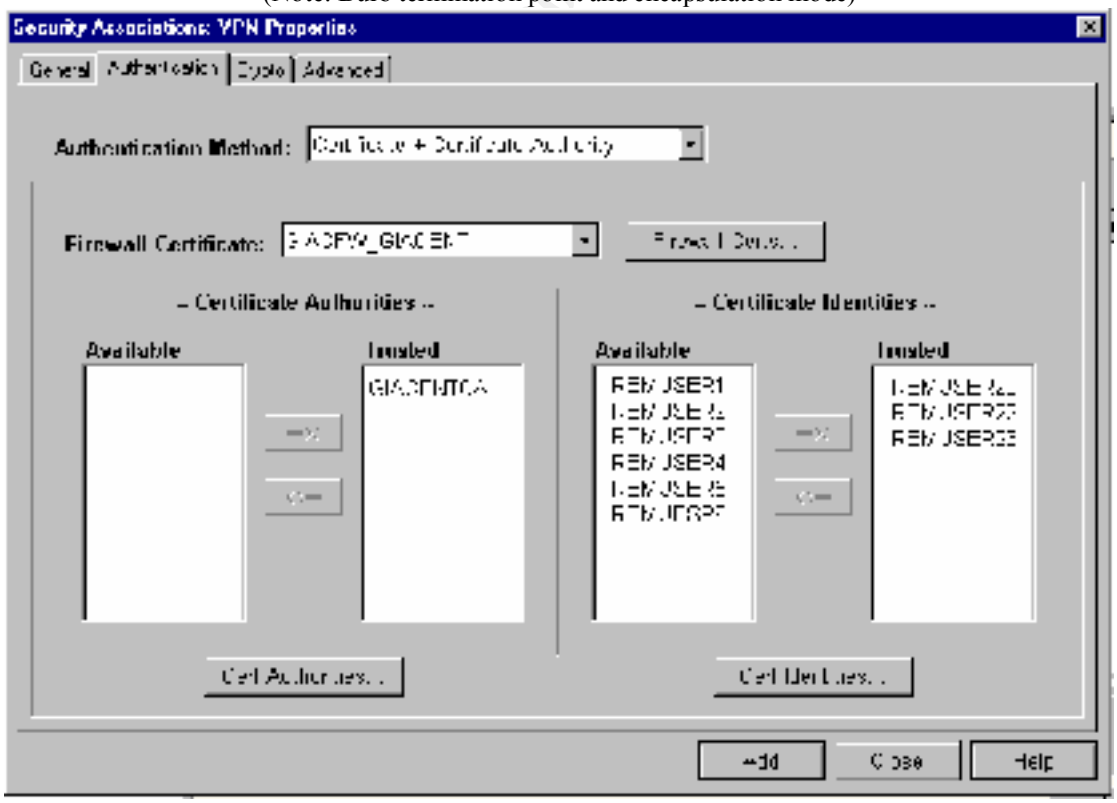


Figure 19. Security Association: Authentication

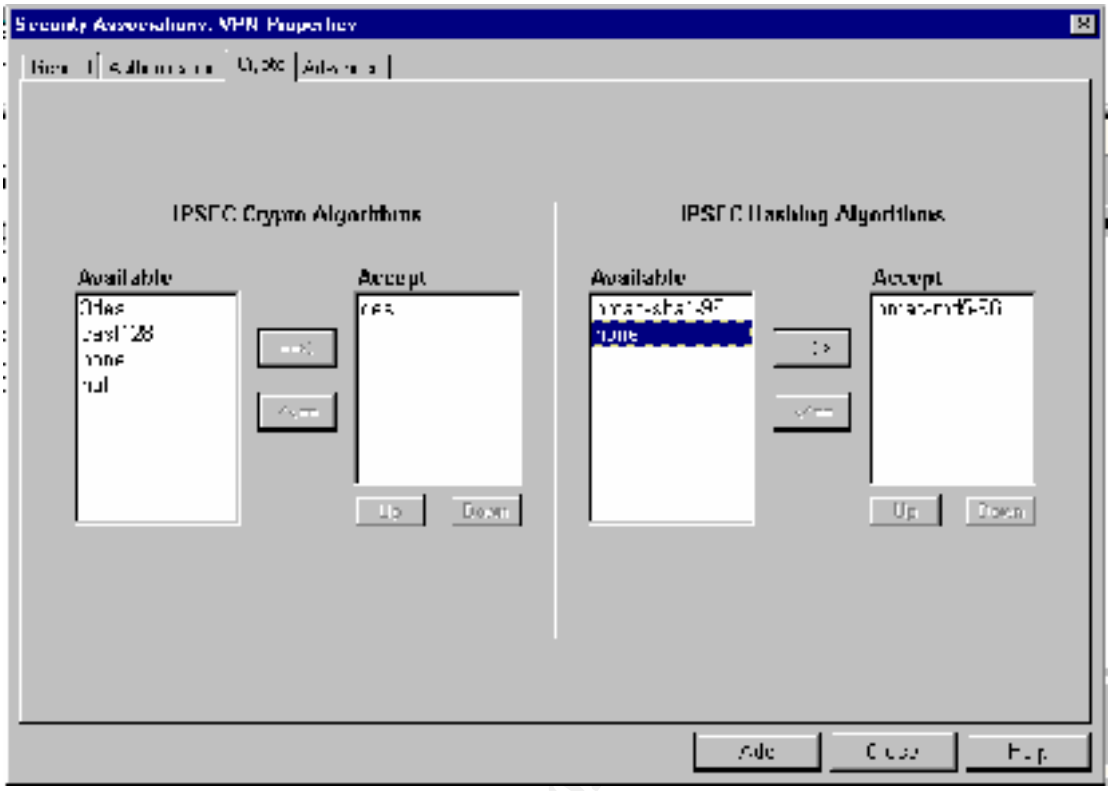


Figure 20. Security Association: Crypto Selection

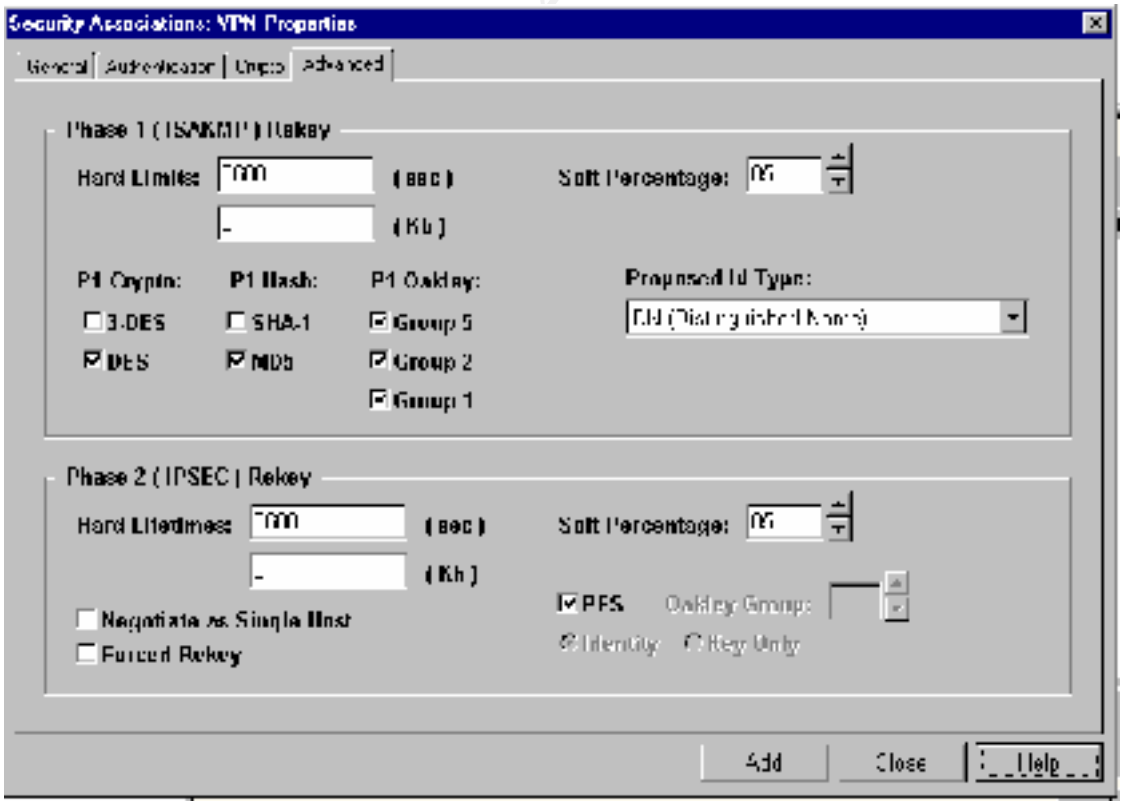


Figure 21. Security Association: Re-key, Crypto, and PFS

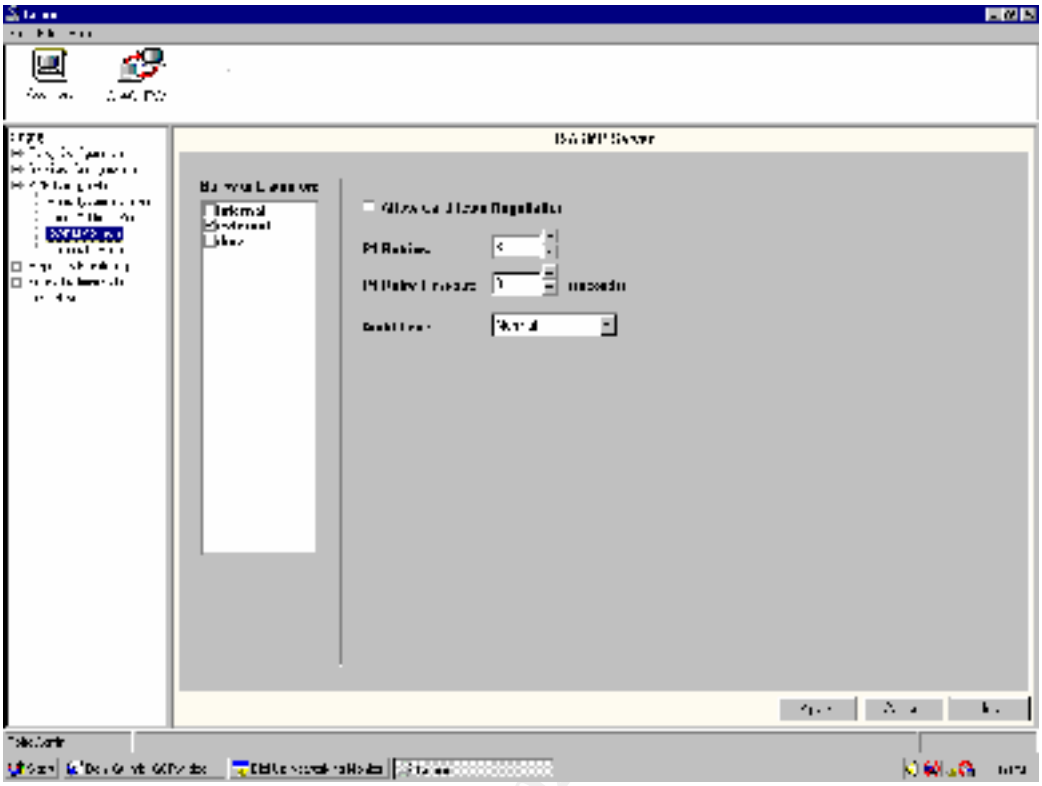


Figure 22 ISAKMP Server
(Note: allow certification negotiation is unchecked for cache/LDAP)

- An ACL must be established for ISAKMP server service. See Figures 23-24.

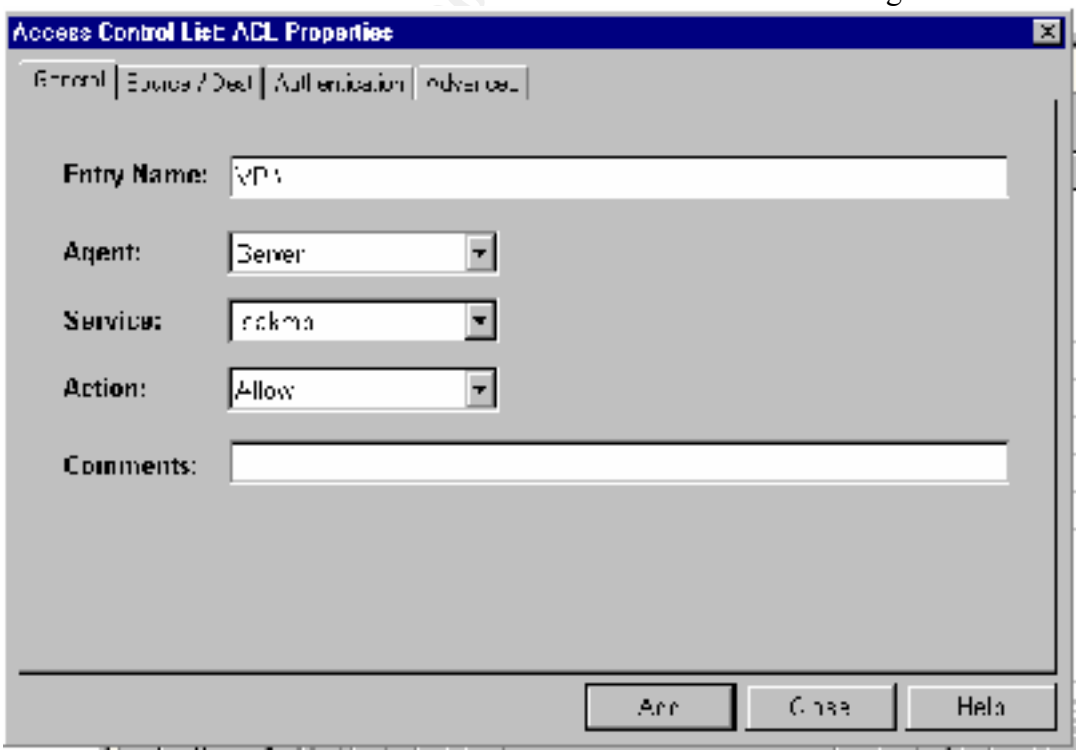


Figure 23. ISAKMP ACL- General

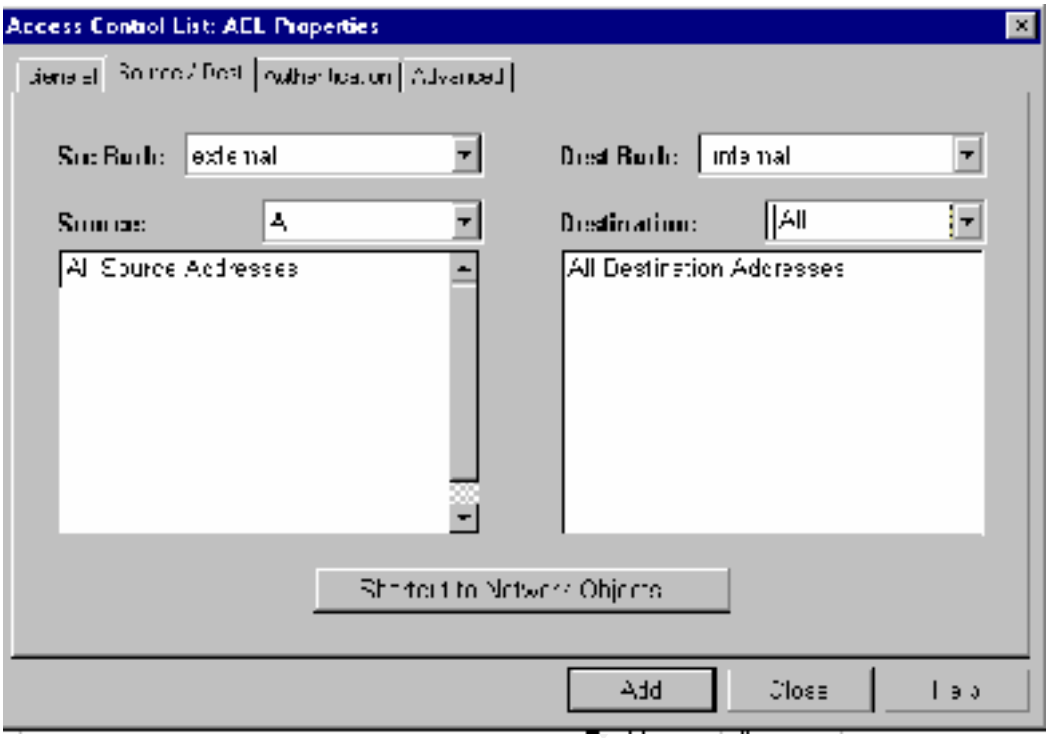


Figure 24. ISAKMP ACL- Source/Destination

SSH Secure Shell

- Secure Shell (tcp, port 22) proxy will be allowed from the PC_GIAC to the EC_GIAC for administrative purposes

Syslog Service

- Syslog (udp, port 514) proxy will be allowed from EC_GIAC Network and the GIAC Enterprises border router's logging interface only.

GIAC Primary Firewall Burb Reference Table:

PC_GIAC	Internet	EC_GIAC
Burb 1	Burb 2	Burb 3
Internal	External	DMZ
Index 1	Index 2	Index 3

GIAC Primary Firewall ACL Order Summary

The following table denotes the preferred order of service checking and the rules imposed on each. Customer access to the e-commerce web server (EC_GIAC Network) is at the highest priority with rules 1 and 2 as it will be the most used service. PC_GIAC Network http/https outbound to the Internet and the EC_GIAC Network is next. (Rules 3 & 4) The internal to external email exchange should be expected to be of fairly high volume so it is positioned as rule 5. Rule 5 is used allow deny all except only authorized mail relays to. DMZ and external syslogging are next (Rules 6 & 7) to support EC_GIAC and GIAC Enterprises border router logging to the syslogger located on the PC_GIAC Network. Rule 8 is for the SSH proxy to the EC_GIAC Network. Rules 9 & 10 allow for all user access to http/https services on the PC_GIAC Network from the PC_GIAC Network. Rule 11 is for remote access via VPN to the PC_GIAC Network. Rules 12, 13, and 14 all

address firewall administration access. Rule 16 denies all other traffic. The exceptions to rule 16 are the DNS, SMTP, and ISAKMP server connections. Their rules are created when these servers are configured.

No	Name	Service	Agent	Action	SrcBurb	Source	DstBurb	Dest
1	http_in	tcp80	proxy	allow	external	*	external	212.212.5.131
2	ssl_in	tcp443	proxy	allow	external	*	external	212.212.5.131
3	http_out_squid	websrvr	server	allow	internal	webusers	external	*
4	http_out_squid	websrvr	server	allow	internal	webusers	dmz	*
5	smtp	tcp 25	server	allow	internal	smtp relays	internal	*
6	syslog	udp514	proxy	allow	dmz	log group1	external	212.212.5.129
7	syslog	udp514	proxy	allow	external	log group2	internal	10.2.1.x
8	ssh	tcp22	proxy	allow	internal	*	dmz	*
9	http_in_loop	tcp80	proxy	allow	internal	*	internal	*
10	ssl_in_loop	tcp443	proxy	allow	internal	*	internal	*
11	isakmp	tcp500	server	allow	external	*	internal	*
12	secureCobra	scobra	proxy	allow	internal	giacadmins	*	*
14	cobra	cobra	server	allow	*	giacadmins	*	*
15	loginconsole	console	server	allow	Firewall	*	Firewall	*
16	deny_all	all	All	deny	*	*	*	*

ACL Summary

GIAC Enterprises VPN Policy

This section will cover the security policy for the GIAC Enterprises VPN. The GIAC VPN will control and manage business partner and supplier access to the SP_GIAC Network. The SP_GIAC Network (10.3.0.0) will be accessible from the Internet via the GIAC Enterprises VPN (212.212.5.130), which is an Intel® NetStructure 3130 Shiva VPN. The SP_GIAC Network will also be administratively accessible via the GIAC Enterprises secondary firewall from the PC_GIAC Network. The Intel 3130 was chosen because of its ability to support IPSEC standards, the Shiva Smart Tunnel (SST) protocol, and its straightforward management approach. Creating VPNS with the 3130 can be summarized as follows:

- Policies are created
- Create a tunnel.

- Assign the appropriate policy to the tunnel (With SST you may create users/groups and assign specific policies)
- Create the access control list to use the tunnel
- Apply network access controls depending on the tunnel termination point (red=trusted, black=untrusted)

Physical Security

- The GIAC VPN will be located in a controlled access area. Only authorized personnel will be granted access.
- Any physical access to the VPN will be by authorized GIAC Enterprises staff and/or vendor maintenance personnel only. Vendor maintenance personnel must have authorized GIAC personnel escort.
- Any maintenance or physical configuration change to the VPN will be by authorized GIAC Enterprises and/or vendor maintenance personnel only. Vendor maintenance personnel must have authorized GIAC personnel escort.
- The VPN console will be located in same controlled access area as the VPN.

Static Configuration Security

- Only personnel designated by the GIAC Enterprises Information Systems Security Officer (ISSO) are authorized to login to the VPN. Authorized personnel with administrator privileges are designated by the ISSO.
- The GIAC Enterprises password policy will be applied for all logins. The password must be at least 8 characters in length, have at least on special character and one capital letter.
- VPN logons are allowed on the local console and the VPN Manager application from the "red network" (SP_GIAC Network).
- The VPN Manager will make use of a local password to protect the VPN Manager configuration file used to communicate to the VPN. The VPN Manager communicates to the VPN via a secure tftp session.
- RMON or SNMP will not be allowed
- The GIAC Enterprises ISSO will review and approve all configuration changes.

Dynamic Configuration Security

- The VPN public key will be valid for 365days before regeneration
- With the exception of IKE negotiation and re-keys, no dynamic configuration is allowed.

Network Services Security

- Two policy groups will be established for VPN management purposes. A policy group for GIAC Enterprises suppliers and a group for GIAC Enterprises partners.
- Suppliers will utilize site-to-site ESP IPSec tunnels that will terminate on the 'black" network (untrusted public network).
- ACLs and proxies will be established to limit suppliers to required services; such as http (tcp 80) access to the SP_GIAC associated Intranet servers.
- Re-keys and renegotiations will be time dependant.

Supplier ESP IPSec Security Profile
(Intel, Creating an ESPv2 IPSec Security Profile)

1. In the File menu of the VPN Manager select New, then Security Profile, then ESP v2 (IKE). The New IKE Profile window appears.
2. In the Profile Name field, enter the name "Supplier" for the IPSec security profile.

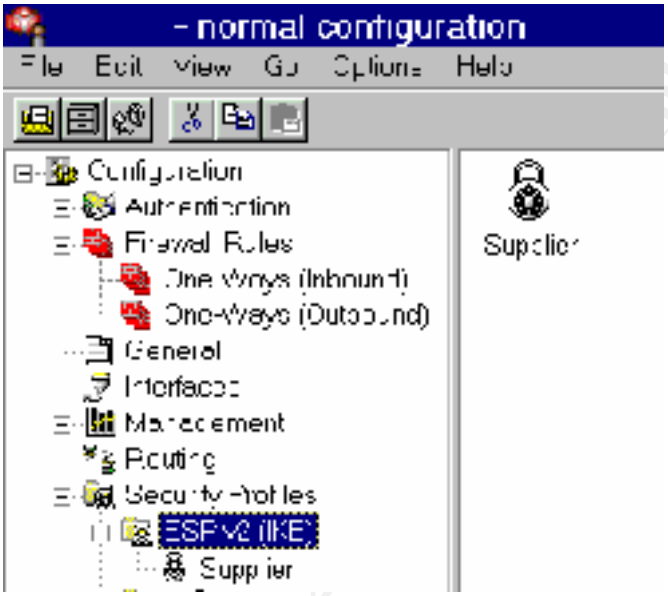


Figure 25. ESP Security Profile#1

3. Click OK. You return to the Configuration window. The new IPSec security profile's icon appears in the left pane and its form view appears in the right pane.
4. In the Authentication field, select the authentication header type: Key *(Note: If you select Key, the authentication method is Challenge Phrase.)*
5. In the Public Key field, select the length, in bits, of the public key used to authenticate the tunnel: 1024 bits *(Note: Intel Network Systems, Inc. recommends using 1024-bit keys. Using the longer 2048-bit keys requires greater computational resources and can degrade system performance. Using 512-bit keys are sufficient if the keys are updated often.)*

- In regards to IPSec configuration, the manufacturers suggestions were followed in most selections. The GIAC Enterprises opted with a time-dependant and kilobytes transferred re-key.

6. In the ESP Algorithm field, select the algorithm 3-DES 168-bit key.
Ensure that the opposing device uses the same algorithm that you specify.
(*Note: Encryption keys with greater numbers of bits provide greater security, but also require greater computational resources, which can degrade system performance. 56-bit DES is sufficient for data that must remain confidential for a*

few days, and 168-bit 3DES can be used for data that requires long periods of security.)

7. In the ESP Authentication field, select the ESP authentication type HMAC MD5
8. In the Authentication Header field, select the authentication header type: HMAC MD5 replay.
9. In the Key Lifetime [time] field, select 12 hours
10. In the Key Lifetime [kbytes] field select 20,480kb

- Next we complete the parameters for IKE. Once again manufacturers suggestions were followed in most selections. The GIAC Enterprises opted with a time-dependant and kilobytes transferred re-key.

11. In the Algorithm field, select the algorithm to use for this profile: 3-DES 168-bit key.
12. In the Authentication field, select the authentication type: HMAC MD5
13. In the Key Lifetime [time] field, select 2 days.
14. In the Key Lifetime [kbytes] field select 20,480kb
15. In the IKE Group field, select the IKE Group 2. *(Note: If you use 3DES, select Group 2 as using Group 1 can weaken the security of your tunnels below 3DES protection.)*
16. Enable tunnel mode for this IPSec security profile, select the Tunnel Mode check box. (*Note: Transport Mode is supported only for IPSec)*.
17. Enable Perfect Forward Secrecy by checking the box
18. Prevent Aggressive Mode, ensure that the Aggressive Mode check box is clear.

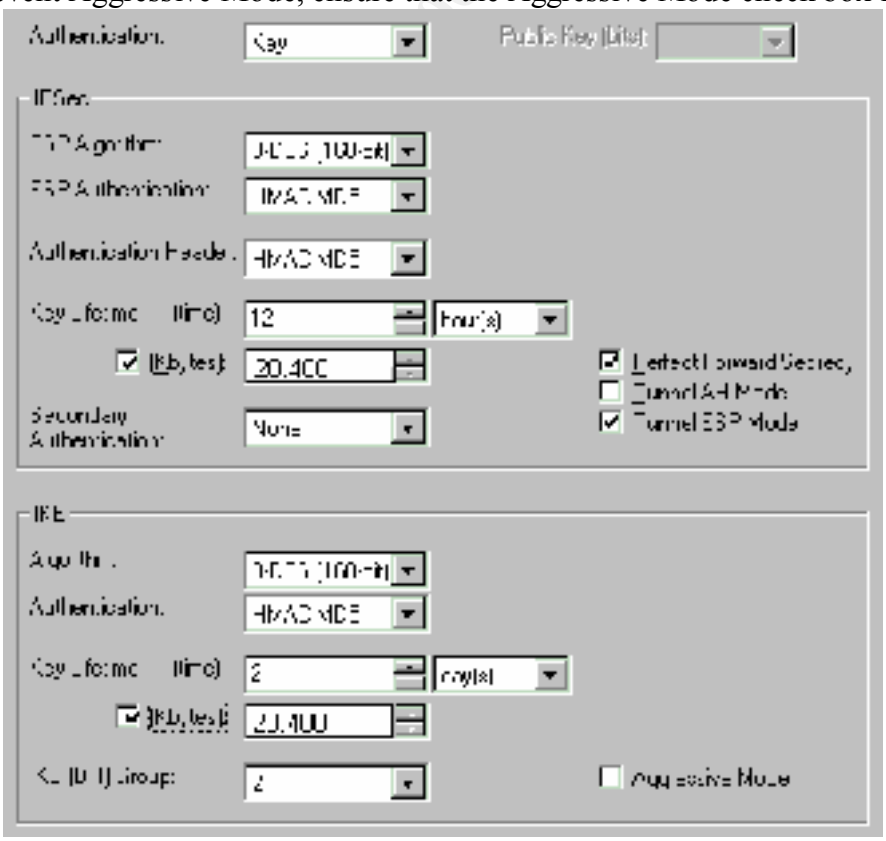


Figure 26. Supplier Security Profile IPSec/IKE

19. Ensure that the Propose Higher Security check box is unchecked.
20. When the configuration changes required are complete, in the File menu, select Save as Text. A confirmation window appears requesting you confirm the configuration change.
21. Click Yes.
22. In the File menu, select Commit, a confirmation window appears requesting you confirm the configuration change.
23. Click Yes. You return to the VPN Manager main window. The Supplier ESP IPSec security profile is available for use immediately.

- All supplier tunnels when created will be assigned the Supplier security profile.
- All Supplier site-to-site tunnels will be configured as peer is master. (GIAC Enterprises operates in listen mode)

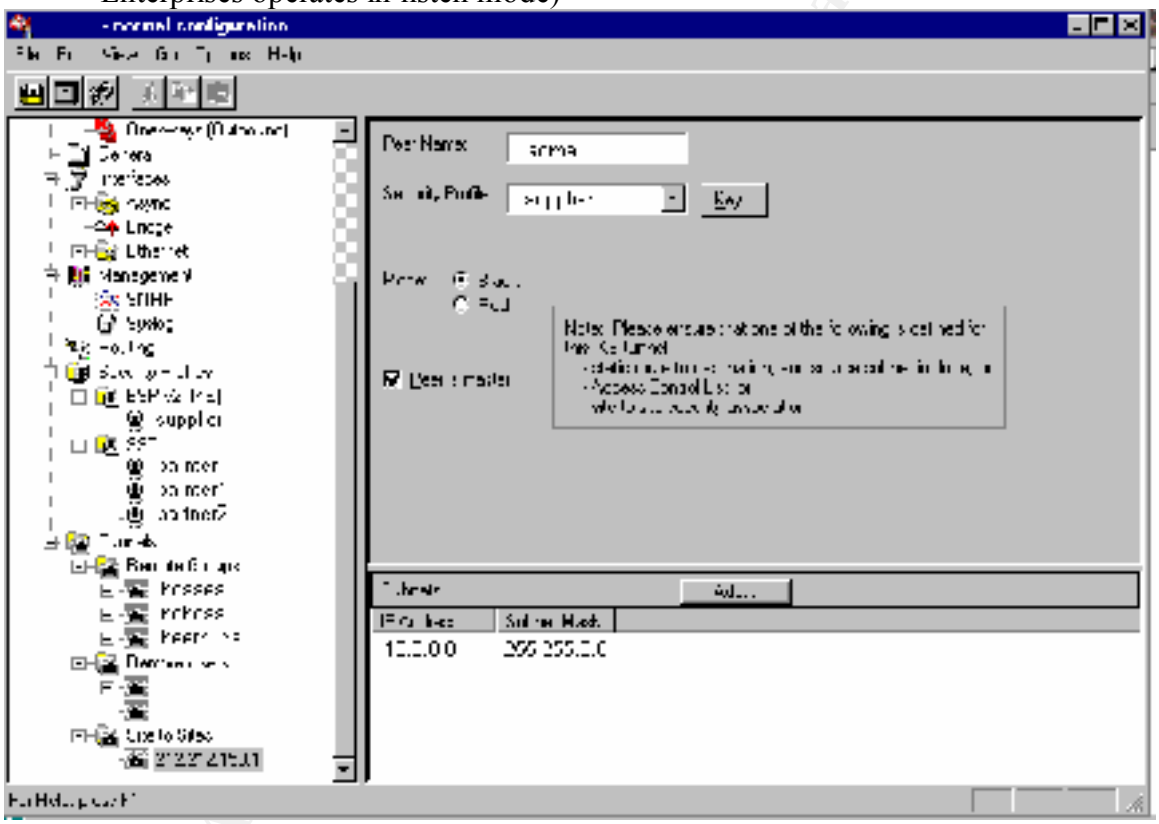


Figure 27. Supplier site-to-site Tunnel Creation

- Challenge phrases will be a minimum of four words or eighteen characters in length.

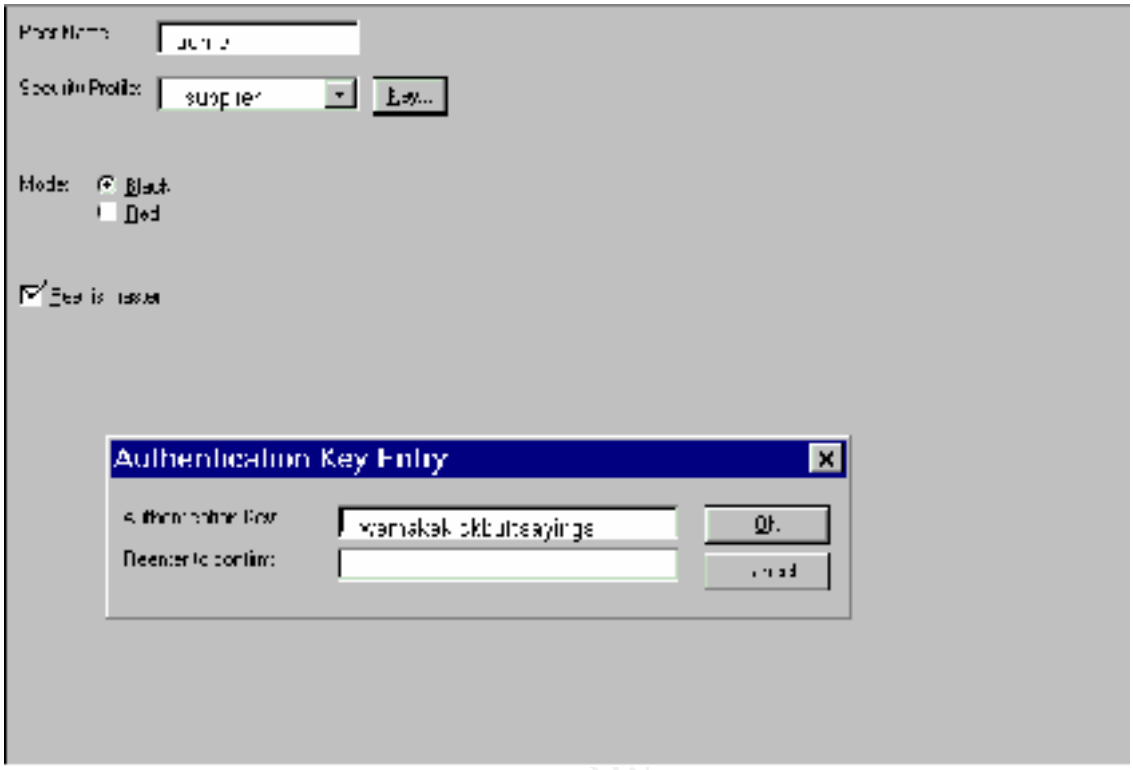


Figure 28.Challenge Phrase Key for Supplier site-to-site Tunnel

- Supplier tunnels will be only be allowed HTTP (tcp 80) to the SP_GIAC Network. This will be accomplished via a stateful proxy setup.

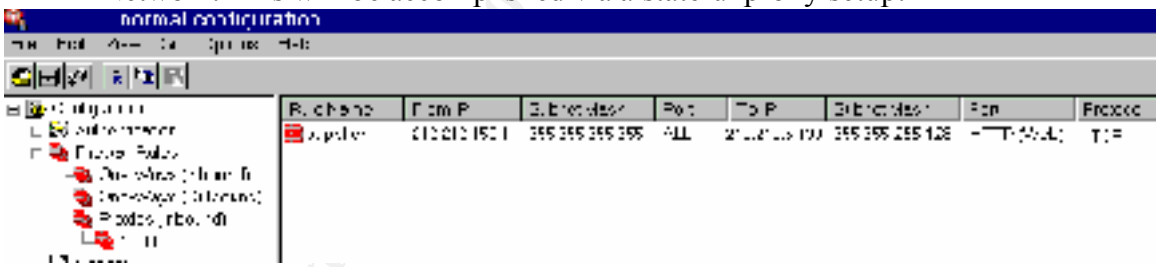


Figure 29. Supplier HTTP Proxy

Partner Shiva Smart Tunnel (SST) Security Profile

- Proprietary tunneling chosen for obscurity.
- Business partners will utilize site-to-site Shiva Smart Tunnels (udp 2233).
- Business partner tunnels will terminate on the "red" network (SP_GIAC Network)
- Business partner access will be limited to the SP_GIAC Network only.
- Business partners will be limited to export limited crypto. (BXA)
- Keys will be regenerated at more aggressive rate of three hours due to the more sensitive nature of the data and use of weaker algorithms.

Creation of the Partner SST security profile is much like the Supplier IPSec security profile with the exception to the following:

1. In the VPN Manager File menu, select New, then Security Profile, and then SST. The New SST Profile window appears.
2. In the Profile Name field, enter Partner. Click OK. You return to the Configuration window.
3. The new SST security profile's icon appears in the left pane and its form view appears in the right pane.

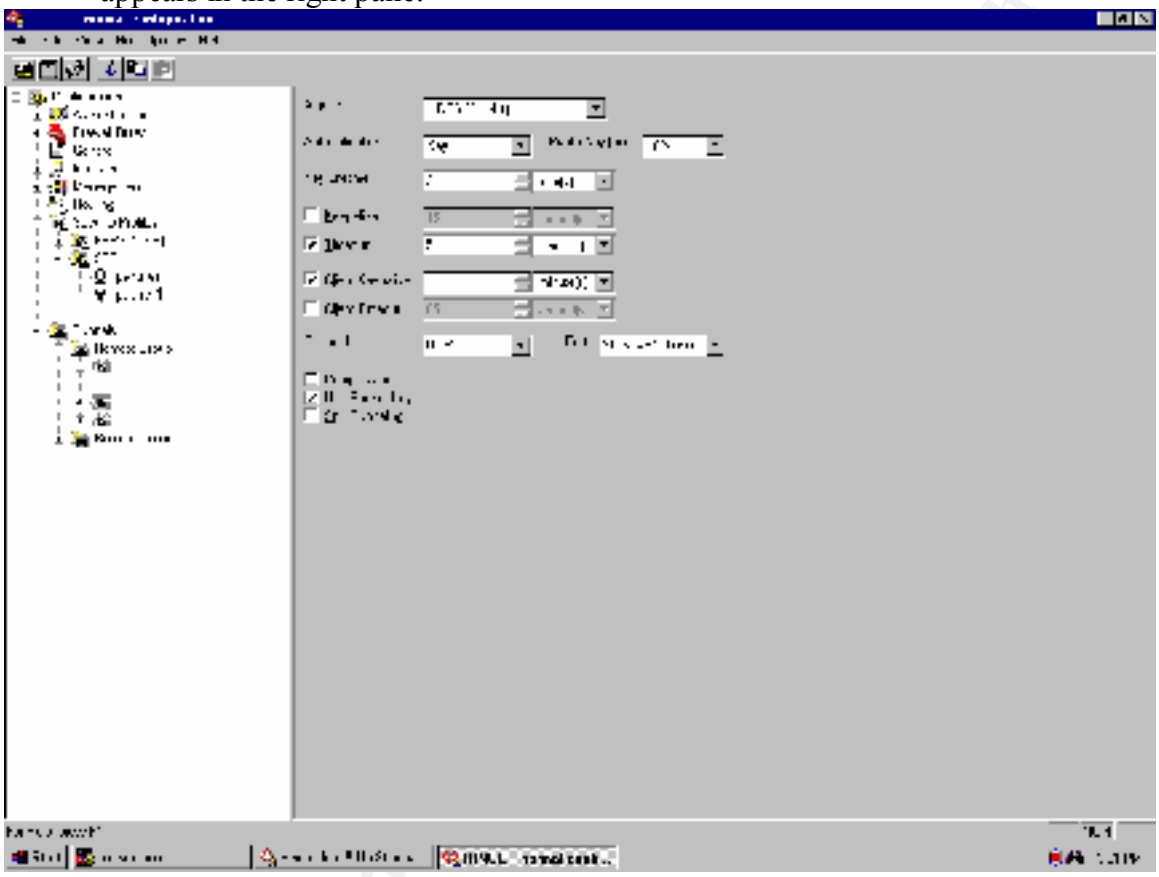


Figure 30. Partner SST Security Profile

4. In the Algorithm field, select the algorithm to use for this profile DES 56-bit key
5. In the Authentication field, select the authentication header type: Key *Note: If you select Key, the authentication method is challenge phrase.*
6. In the Public Key field, select the length, in bits, of the public key used to authenticate a tunnel: 1024 bits *(Note: Intel Network Systems, Inc. recommends using 1024-bit keys. Using the longer 2048-bit keys requires greater computational resources and can degrade system performance. Using 512-bit keys is sufficient if the keys are updated often).*
7. In the Key Lifetime [time] field, select 3 hours until the session keys should be renegotiated.
8. Keepalive settings are can be site specific due to latency and other issues. Trial and error required here.
9. Set the Timeout check box and set the timeout to 5 minutes. If the GIAC VPN doesn't receive any Keepalive signals for 5 minutes, the security association with the corresponding tunnel is dropped.
   This selection enables the Timeout duration fields.

10. Specify UDP traffic, accept the default selection of UDP in the Protocol field.
11. In the Port field, accept the default displayed, Shiva SST VPN Tunnel (udp 2233)
12. Enable LZS compression for the Partner SST security profile for performance enhancements.
13. Enable the use of a packet key to encrypt/decrypt the SST packets, select the Packet Key check box. *(Using the session key to encrypt packets reduces the number of per-packet encryption operations to one from two, which may increase throughput but reduce security)*
14. Prevent cleartext traffic from proceeding to the local network (the default state), disable split tunneling by clearing the Split Tunneling check box.

- Partner site to site tunnels and assign the Partner security profile

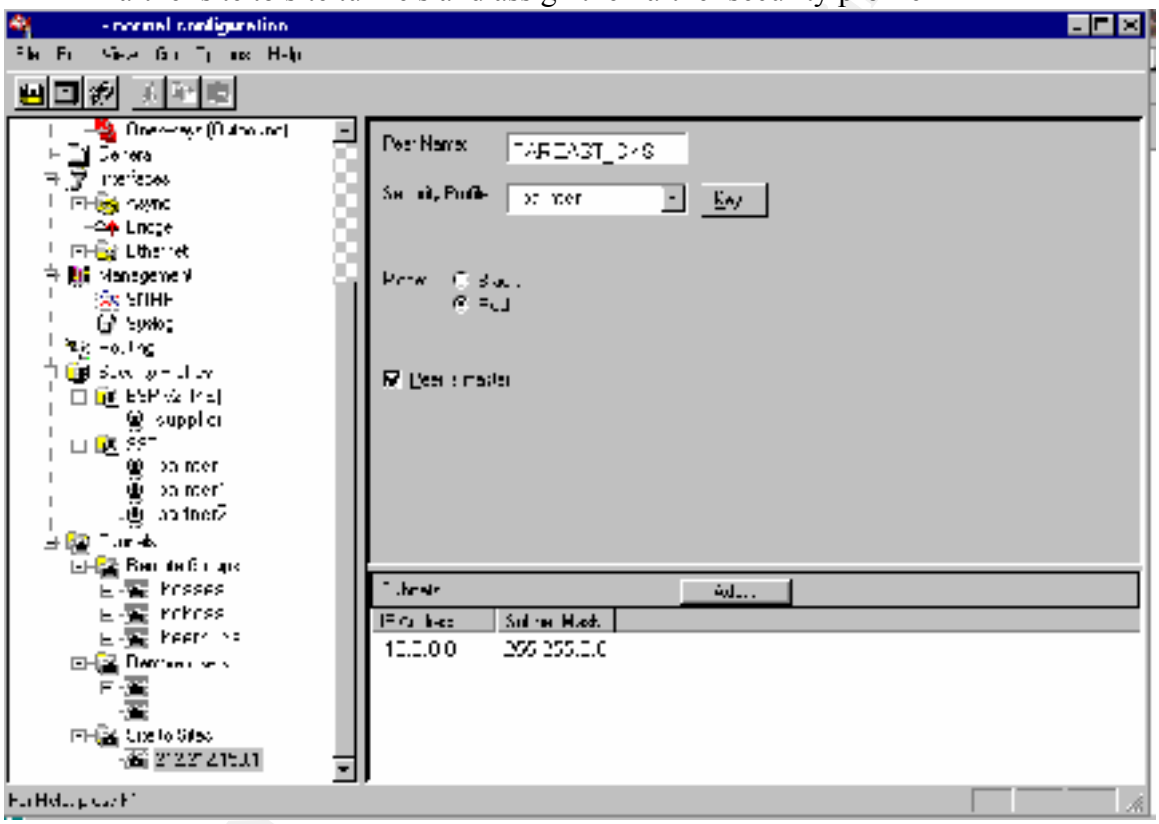


Figure 31. Partner SST Tunnel

- VPN logging will be directed to the VPN console and syslogger (level6) located on the PC_GIAC Network

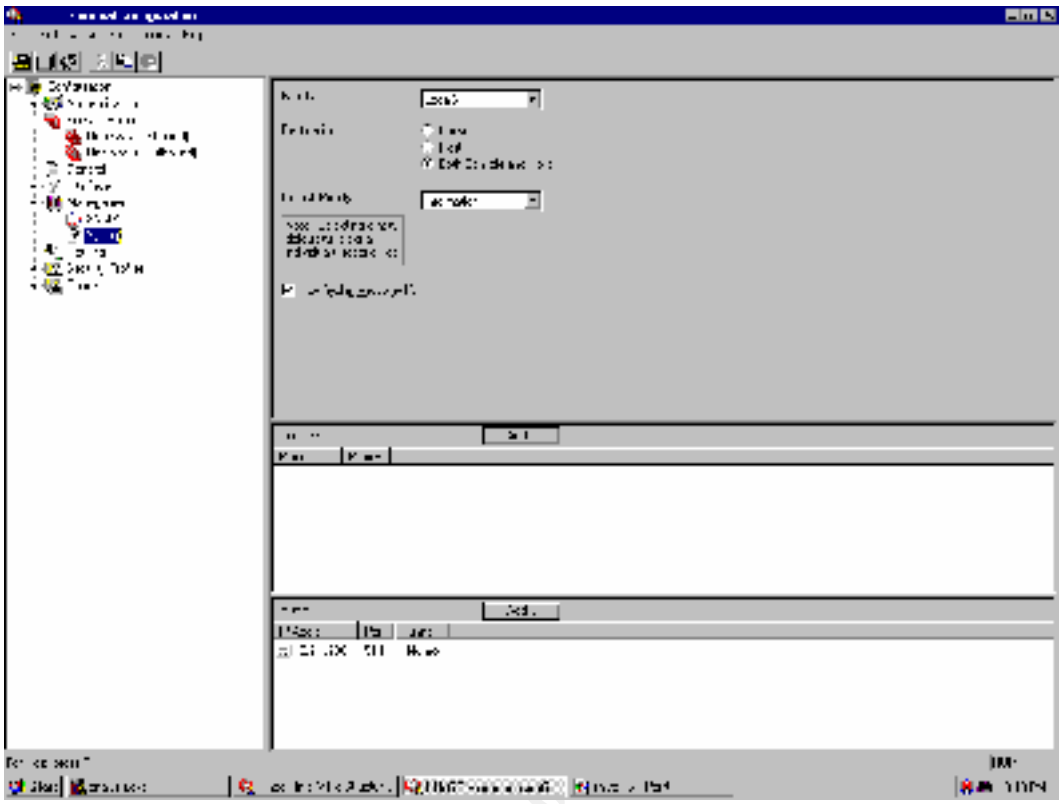


Figure 32. GIAC VPN Logging

- The GIAC VPN will utilize the SP_GIAC Networks DNS, DHCP, and WINS servers.

Assignment Three: Auditing the Architecture

In this section an assessment and audit of the GIAC Enterprises perimeter architecture will be constructed with special focus being placed upon the primary firewall.

Planning and Reasoning

The audit and assessment will be done primarily to insure the GIAC Enterprises primary firewall policy implemented is indeed being enforced. The audit will also help to discover any possible weaknesses and also give insights to expected responses of typical and non-typical events.

Things the assessment will check and what tools/commands used:

- Scanning to see what network services are available: Nmap2.53, ping command.
- ACL checking for restricted services: Telnet, netcat, or a web browser
- Information leakage through web proxies: web based proxy check All Nettools.com
- Information leakage through DNS: nslookup command
- Mail relaying: web based anti-mail relay check Pacific Internet Limited

In planning the part of an assessment that places network load or excessive traffic (such as scanning) on the a device, a two step process should be considered:

- The first should be planned off-hours during what could be expected as a network "quiet" time. (e.g. very early Monday A.M.) This will support two things, non-

disruption of business operations and the also make it easier to witness/review expected and non-expected stimulus and responses. This is a least cost effort as it minimizes risks and could be completed in a few hours.

- A second assessment should also be planned during a known network "normal" time. This step also supports two things, load/stress testing against the policy (does it break or behave differently under a load?) and it also enables us recognize what events or expected responses we will see when the network is experiencing such stimuli or an attack. The overall risk of this step should be considered as testing or antagonizing a network under full load can lead to unpredictable results. The second assessment also requires more preliminary work to gather information from firewall traffic reports, sysloggers, etc. to have a good understanding of what expected normal load and traffic is. This total time for reviewing, planning, and implementing could actually take a few days if not possibly a week or more.

Due to the assumptions of the GIAC Enterprises assessment, only the first step will be covered.

Assessment Implementation

The first step of the assessment it to look for any undesired ports that may be open and to verify expected to results on all interfaces of the firewall. This will be accomplished utilizing the Nmap tool and running UDP, TCP SYN, NUL, and FIN scans against all interfaces and recording the results. ICMP responses on the firewalls external interface are against policy so that will be checked also with ping command.

Ping Test

Verify the external interface doesn't respond to ICMP requests.

giacdude$ ping -n 212.212.5.129
PING 212.212.5.129 (212.212.5.129): 56 data bytes
^C
--- 212.212.5.129 ping statistics ---
163 packets transmitted, 0 packets received, 100%packet loss

Nmap Scans

Nmap scans against firewalls external interface from the DMZ. Results follow each command.

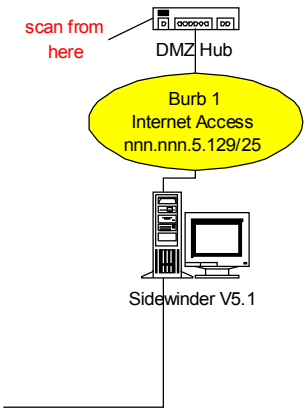


Figure 33. DMZ and external interface

The first command runs a SYN scan against Nmap default ports, don't ping the target, fragment packets, and don't resolve the hostname, and save the results to a file.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -P0 -f -n -oN ./fw_sSP0foN 212.212.5.129
Interesting ports on (212.212.5.129):
(The 1518 ports scanned but not shown below are in state: filtered)

Port	State	Service
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https
500/tcp	open	isakmp

 # Nmap run completed -- 1 IP address (1 host up) scanned in 877 seconds

The next command runs a FIN scan against Nmap default ports, don't ping, fragment packets, and don't resolve the hostname, and save the results to a file.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -sF -P0 -f -n -oN ./fw_sFP0fnoN 212.212.5.129
All 1523 scanned ports on 212.212.5.129 are: closed
 # Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds

The next command runs a NULL scan against Nmap default ports, don't ping, fragment packets, and don't resolve the hostname, and save the results to a file.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -sN -P0 -f -n -oN ./fw_sNP0fnoN 212.212.5.129
All 1523 scanned ports on (212.212.5.129) are: closed
 # Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

The final scan to this interface runs a UDP scan against Nmap default ports, don't ping, don't resolve the hostname, and save the results to a file.

Nmap -sU -P0 -n -oN ./fw_sUP0oN 212.212.5.129
Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Interesting ports on (212.212.5.129):
(The 1447 ports scanned but not shown below are in state: filtered)

Port	State	Service
514/udp	open	syslog

Nmap run completed -- 1 IP address (1 host up) scanned in 1743 second

The next group of Nmap scans will be from the internal burb PC_GIAC Network with the same rules applying to each.

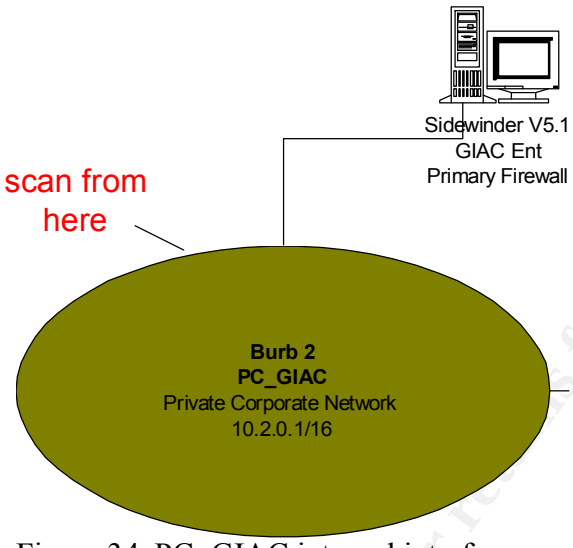


Figure 34. PC_GIAC internal interface

The first command runs a SYN scan against Nmap default ports, don't ping the target, fragment packets, and don't resolve the hostname, and save the results to a file.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -P0 -f -n -oN ./fw2_sSP0foN 10.2.0.1
Interesting ports on (10.2.0.1):
(The 1515 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https
3128/tcp	open	squid/http
9002/tcp	open	unknown
9003/tcp	open	unknown

 # Nmap run completed -- 1 IP address (1 host up) scanned in 877 seconds
NOTE: 9002 and 9003 are the cobra admin ports and secure cobra proxy.

The next command runs a FIN scan against Nmap default ports, don't ping, fragment packets, and don't resolve the hostname, and save the results to a file.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -sF -P0 -f -n -oN ./fw2_sFP0fnoN 10.2.0.1
All 1523 scanned ports on 10.2.0.1 are: closed
 # Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds

The next command runs a NULL scan against Nmap default ports, don't ping, fragment packets, and don't resolve the hostname, and save the results to a file.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -sN -P0 -f -n -oN ./fw2_sNP0fnoN 10.2.0.1
All 1523 scanned ports on (10.2.0.1) are: closed
 # Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

The final scan to this interface runs a UDP scan against Nmap default ports, don't ping, don't resolve the hostname, and save the results to a file.
Nmap -sU -P0 -n -oN ./fw2_sUP0oN 10.2.0.1
Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Interesting ports on (10.2.0.1):
All 1448 scanned ports on (10.2.0.1) are: closed
Nmap run completed -- 1 IP address (1 host up) scanned in 1723 second
The final group of Nmap scans will be from the DMZ burb (EC_GIAC Network) with the same rules applying to each.

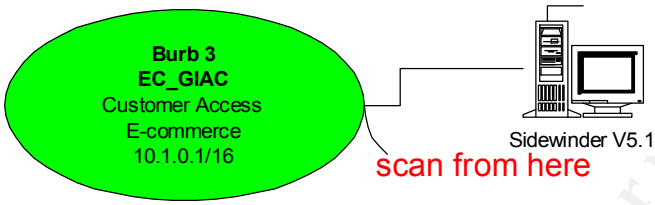


Figure 35. EC_GIAC dmz interface

The same series of scans are run with all the results returning no open TCP or UDP ports.
Conclusion
Test results on all interfaces were as expected and favorable.

ACL verification
The next step is to verify the ACL groups that have been defined for specific services. Testing will be accomplished by using hosts that are not assigned to ACL groups for the services HTTP, HTTPS, SSH, Sendmail, Cobra, and Secure Cobra.

1) *HTTP/HTTPS ACL Check*

When attempting to access the Internet or EC_GIAC Network via a web browser using HTTP/HTTPS from the PC_GIAC Network. The following is displayed.

Error 403
ERROR
Access Denied

The following error was encountered:
Access Denied.
If you feel you have reached this message in error please contact your system administrator for further assistance

2) *SSH ACL Check*

When attempting to connect to EC_GIAC Network host from unauthorized PC_GIAC host.
 # ssh 212.212.5.131
connect closed by remote host.

3) *Sendmail ACL Check*

The GIAC primary firewall's internal Sendmail ACL for SMTP traffic will only accept mail from the GIAC Enterprises authorized mail exchange host. Using the telnet command to port 25 from any host will verify this.
#telnet 10.2.0.1 25
telnet unable to connect connection refused..

4) *Cobra and Secure Cobra ACL Check*

Verifying ACLs for the Sidewinder management programs Cobra and Secure Cobra can be accomplished by using the telnet command to the appropriate ports.
#telnet 10.2.0.1 9002
telnet unable to connect connection refused..
#telnet 10.2.0.1 9003
telnet unable to connect connection refused..

DNS Zone Transfer Check

To insure that only external burb (public) DNS information is shown to the Internet community. Connect to the external burb's DNS server and perform a zone transfer and review the results.

```
admin$ nslookup
Default Server:  giacfw.giacent.com
Address:  212.212.5.129
> set type=any
> ls –t  giacent.com > giaczone
received  9  records
> quit

admin$ cat giaczone
giacent.com     SOA     giacent.com hostmaster.giacfw.giacent.com. (9 172800 3600 1728000 172800)
giacent.com     NS      giacfw.giacent.com
giacent.com     MX      giacfw.giacent.com
giacent.com     MX      5       giacfw.giacent.com
giacvpn         A       212.212.5.130
www             A       212.212.5.131
localhost       A       127.2.0.1   <<NOTE required for forward lookups from internal burb>>
giacfw          MX      10 giacfw.giacent.com
giacent.com     SOA     giacent.com hostmaster.giacfw.giacent.com. (9 172800 3600 1728000 172800)
```

Conclusion: The results are satisfactory

Mail Relay Check

Although mail relaying is not considered a drastic security risk, if not prevented it can attribute to SPAMing from the GIAC Enterprises domain and rob the firewall of resources.
The online test site used is: Pacific Internet Limited

```
Escape character is '^]'.
220 giacfw.giacent.com ESMTP Tue, 14 Aug 2001 18:30:38 -0400 (EDT)
helo nocops.pacific.net.sg
250 giacfw.giacent.com Hello nocops.pacific.net.sg [203.120.74.3], pleased to meet you
mail from: noc1@hk.super.net
```

250 noc1@hk.super.net... Sender ok
rcpt to: alanb@kirchhoff.pacific.net.sg
550 alanb@kirchhoff.pacific.net.sg... Relaying denied

Conclusion: Results are good. Internet burb Sendmail doesn't relay.

Web Proxy Check
Using a browser on an Internet authorized machine and utilizing the All-Nettools web site for proxy check. We are returned the desired results.

Proxy Detected
giafw.giacent.com 212.212.5.129
giafw.giacent.com 212.212.5.129

No internal hostname or IP is passed through the proxy.

Conclusions
Overall the initial assessment was favorable. There were no surprises and the firewall is doing exactly what it was asked to. There are some still some improvements that could be made. The implementation of a more robust authentication system; such as a RADIUS, SNK server or the use of certificates on the PC_GIAC Network would compliment the firewall ACLs with a higher level of assurance of access controls. Implementation of an IDS system of onto the three networks would also be desired.

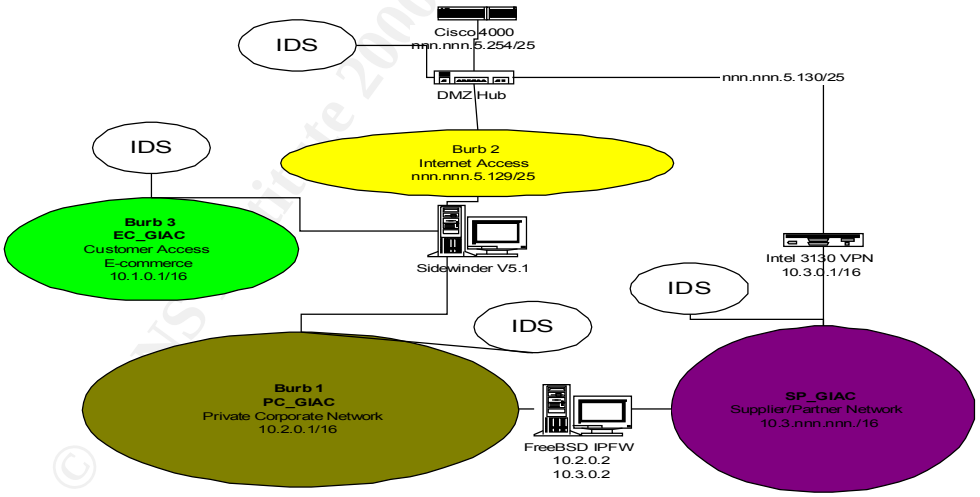


Figure 36.GIAC Enterprises Reconsidered

Assignment Four: Design Under Fire

The design chosen for attack is Brian Rickle, from Capital SANS 2000. http:///www.sans.org/y2k/practical/Brian_Rickle_GCFW.zip,

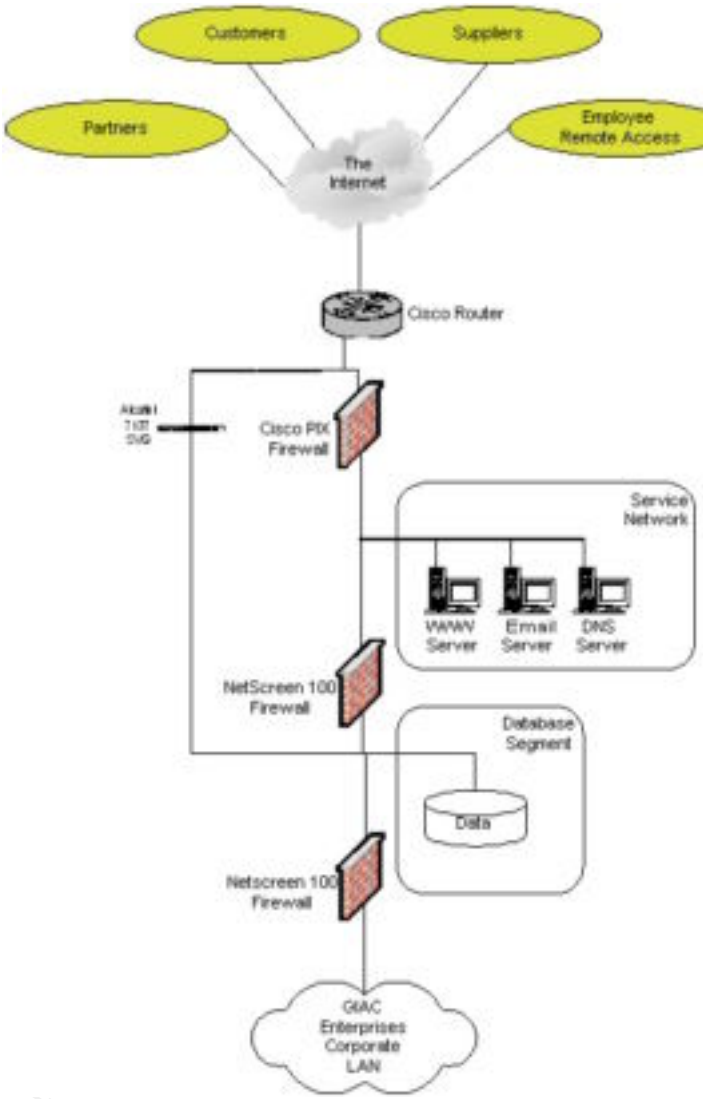


Figure 37.

Firewall Attack

The primary firewall in the above architecture is Cisco PIX 525 (Rickle, p7) and will be the intended victim.

The attack planned (gain access, escalate privilege, and pilfer) (ScambrayMcClureKurtz, rear cover) will use a known flaw in the Mailguard feature on the firewall. The Mailguard filter fails to check for strict sequence of SMTP commands making it possible to pass data through the firewall to the "protected" SMTP server located behind the firewall. To elaborate, generally there is a set sequence of SMTP commands that take place when an email exchange occurs:

HELO or EHLO
MAIL FROM: scriptkiddie@hackeru.org
RCPT TO: You2@giacent.com
DATA
<message>

The flaw in the Mailguard filter allows the DATA command to be accepted first, thus using a tool such as netcat we may pipe scripts and data to the target server to gain access and establish our toehold.

netcat –v –v mail.giacent.com 25 < myfavsendmailexploit

- The Mailguard vulnerability is listed under CVE-2000-1022 (CVE, Mitre Corp) with details at 2000-09-19: Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability (Securityfocus) and http://ciac.llnl.gov/ciac/bulletins/l-002.shtml (CIAC)

Once toehold has been achieved then the mail server itself will be employed to complete the attack against the firewall. The attack used directly against the firewall will be a Denial of Service attack created by a flaw in the TACACS+ authentication server. By submitting a large number of bogus authentication requests to the TACACS+ server and the server not being able to properly handle them severely impacts operation and can possibly crash the firewall.

- The TACACS+ vulnerability is listed under CAN-2001-0375 (CVE, Mitre Corp) with details at Securityfocus 2001-04-06: Cisco PIX TACACS+ Denial of Service Vulnerability

.

DoS Attack

Given the scenario of fifty comprised cable modem/DSL systems at use against the given architecture Cisco 4000 with a 10mb service (Rickle, p13) any flood of the network would have an undesired effect even with the filtering Mr. Rickle has in place.

- A course of action to alleviate TCP SYN may be to configure TCP Intercept on the router. (http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm)(Cisco).
- Another possibility on how to reduce the effects is by setting Committed Access Rate (CAR), but given the bandwidth involved that may still be futile.
- Implementation of IDS systems that will perform automatic resets during TCP SYN floods to the hosts being attacked may help alleviate stress on those systems. (ScambrayMcClureKurtz, p493)

System Compromise

Reconnaissance of the network utilizing whois, nslookup, and other public sources provide information about the target network. Reading the source code of the targets public web pages can sometimes provide valuable information. This preliminary

intelligence gathering can all be done without a suspicious or malicious packet being sent. After the dissemination of the information the target is the e-commerce server. Reasons are as follows:

- A web server more than likely improves my chances of success.
- The server supports SSL so the possibility also exists that some of the exploits I exercise can be via SSL tunnel making them impossible for IDS systems to spot.
- It being an e-commerce box, it is probably administrated heavily given the possibility of more likely any activity to be lost in the shuffle and better opportunities to capture other administrator passwords.

The next step is to determine what platform and web server is in use. This can be accomplished with netcat .

netcat –v -v www.giacent.com 80
GET
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Thu, 1 Aug 2001 05:16:47 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>sent 6, rcvd 224: NOTSOCK

Now that the web server type has been determined, known root or admin privilege gaining exploits can be exercised against it. SUBJ is an automated tool that scans for many known IIS related vulnerabilities and also a variety of cgi script vulnerabilities.

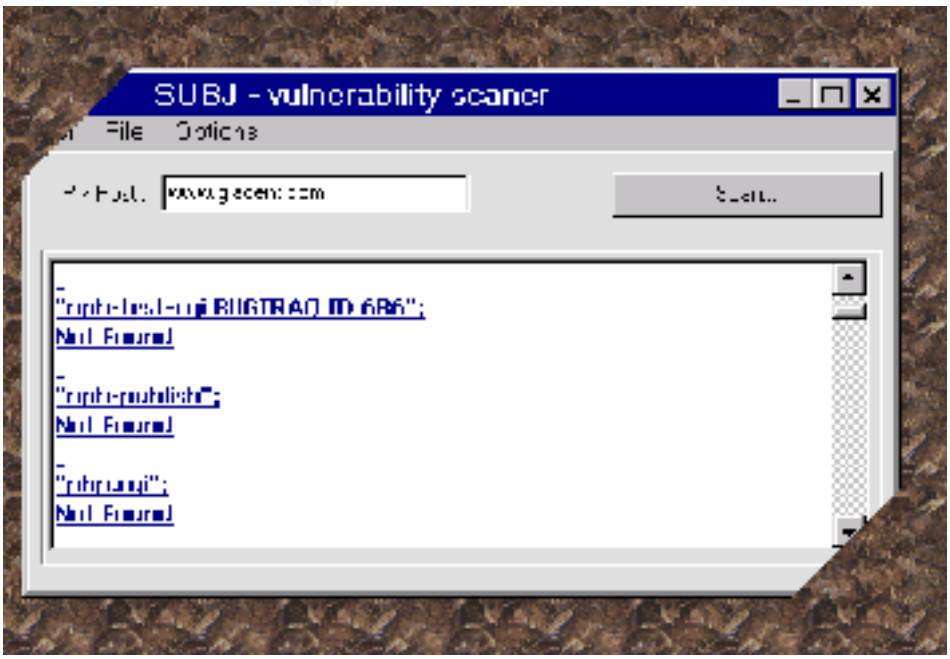


Figure 38. SUBJ Vulnerability Scanner

[cut of SUB output]
"showcode.asp#2";
<<<----------[Exists!!!]----------->>>
Reference: http://www.securityfocus.com/vdb/?id=167

"ss.cfg";
Not Found

"get32.exe BUGTRAQ ID 770";
<<<----------[Exists!!!]----------->>>
Reference: http://www.securityfocus.com/vdb/?id=770

The get32.exe is the jackpot winner.
http ://victim.com/cgi-bin/get32.exe|echo%20>c:\file.txt
This will overwrite file.txt, or any file you specify. The get32.exe program will also allow the injection of code bytes into any executable file.

http ://www.victim.com/cgi-bin/alibaba.pl|dir
This will provide a directory listing of the CGI directory.

http ://www.victim.com/cgi-bin/tst.bat|type%20c:\file.txt
This will display the contents of file.txt

- /data/vulnerabilities/exploits/AlibabaFileOverwriteXploit.c

MISSION ACCOMPLISHED!!

References:

1. National Security Agency, "Router Security Configuration Guide", April 20,2001, Version 1.0g http://nsa1.www.conxion.com/cisco/download.htm, Aug 10, 2001
2. Brenton, Chris, "Firewalls 102: Perimeter Protections and Defense In Depth", SANS Baltimore, May 2001
3. Secure Computing Corporation, "Sidewinder™ Version 5 Administrators Guide", March 2000, SWOP-MN-ADM50-A
4. Intel Corporation, "Intel® NetStructure VPN Manager Guide", 2000
5. BXA Encryption Export Regulations, Jan. 12, 2000, http://www.eff.org/Privacy/ITAR_export/2000_export_policy/20000112_cryptoexport_regs.html, Aug 10, 2001
6. Scambray, Joel; McClure, Stuart; Kurtz, George; "Hacking Exposed Second Edition", ISBN 0-07-217748-1, 2001 Osborne/McGraw-Hill
7. NMAP2.53beta, Fyodor@dhp.com, http://www.insecure.org/nmap/index.html, Aug 10, 2001
8. Proxy check, http://www.all-nettools.com/tools1.htm, August 14, 2001

9. Pacific Internet Limited, Network Operations Center, Online Mail Relay check, http://nocops.pacific.net.sg/serviceLink/mailrelaycheck.html, Aug 14, 2001
10. netcat, http://www.l0pht.com/~weld/netcat/, Aug 14, 2001
11. Brian Rickle, http:///www.sans.org/y2k/practical/Brian_Rickle_GCFW.zip, Aug 14,2001
12. CVE, Mitre Corp. http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=pix, Aug 14, 2001
13. Securityfocus.com, http://www.securityfocus.com/frames/?content=/forums/bugtraq/intro.html, Aug 14, 2001
14. CIAC http://ciac.org/ciac Aug 14, 2001
15. Cisco, http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm, Aug 14,2001
16. SUBJ, mailto: lis_cpc@mail.ru. Apologies for not providing more information. This is a difficult tool to locate and was pulled from a local archive.