Global Information Assurance Certification Paper

GIAC Enterprises: Network Security Architecture

GCFW Practical Version 1.7
SANS Monterey, 2002

By

Tim Ghebeles
August 20, 2002

BACKGROUND -- GIAC Enterprises

GIAC Enterprises of San Francisco, California, is a newly formed e-business selling online fortune cookie sayings. Their business reseller partnership includes Fortune411, based in Singapore. They recently signed fortune supplier agreements with Tokyo based Wonton Words, and London based 4Tuna, Ltd.

GIAC is a small company with 20 employees. Because of current market demand, GIAC has requested a secure enterprise network solution that will meet existing business requirements, while allowing for future business growth.

E-BUSINESS REQUIREMENTS

GAIC Enterprises has the following e-business service requirements:

CUSTOMER REQUIREMENTS

Customers need access to GIAC public services (web, dns, email) for general corporate information and e-communication. They will be using https via www.giac.com to do order management (submit, update, cancel, and order status).

SUPPLIER REQUIREMENTS

Suppliers Wonton Words, and 4Tuna, Ltd., need access to GIAC public services (web, dns, email) for general corporate information and e-communication. They will need secure access to the supplier services network in order to deliver fortune text files to the fortune repository FTP server, and the secure supplier management interface www.suppliers.giac.com via https.

PARTNER REQUIREMENTS

Business partner Fortune411, needs access to GIAC public services (web, dns, email) for general corporate information and e-communication. Fortune411 will need secure access to the partner services network in order to access the partner fortune download server, and the secure partner management interface www.partners.giac.com via https .

GIAC EMPLOYEE REQUIREMENTS

GIAC employees require access to corporate services including intranet web, dns, email, printer, and file sharing services. They also require external web access, which will be provided via a Squid http proxy server. Employees may be on-site, remote, or telecommuting.

OPERATIONAL REQUIREMENTS

Flexibility

GIAC Enterprises requires a flexible network design. This will allow GIAC to respond to market forces and add additional network capacity and/or firewalls in order to meet dynamic business requirements.

Maintainability

GIAC requires a simple and supportable network security architecture. The current IT market has made it hard to retain good IT support staff. It is imperative that the network design will be able to be maintained and supported by a minimum IT skill set.

Network Throughput

GIAC has signed a service contract with a local ISP CloudNine, providing T1 connectivity. The ISP service agreement will allow GIAC to upgrade to a higher throughput connection. This upgrade will be driven by market demand.

NETWORK SECURITY DESIGN METHODOLOGY

A robust network security design must meet the three fundamental InfoSec criteria: confidentiality, integrity, and availability (CIA). These criteria will be used as a baseline for establishing the appropriate controls and safeguards necessary to minimize network security threats and vulnerabilities.

The following design strategies will be used to minimize risk exposure for GIAC Enterprises e-business:

Defense In-Depth

Defense in-depth is a design strategy that utilizes multiple network components in order to

provide concentric, redundant layers of protection. The GIAC Enterprises design will use both a border router, and a perimeter vpn/firewall in order to enforce the appropriate access controls for risk mitigation. This design balances the business need for a maintainable network architecture, with the minimum components needed for defense in-depth protection.

Configuration Hardening

Configuration hardening is the process of locking down and securing the various network components in order to reduce vulnerabilities. The GIAC Enterprises design will address the router/firewall operating system, application, and network service levels in order to ensure CIA compliance.

Compartmentalization

GAIC IT assets will be classified and segregated based on business function, risk, and asset valuation. The network architecture will follow directly from this classification. This will ensure GIAC Enterprises can monitor, contain, and minimize collateral damage due to a compromise.

Security Policy Stance

The GIAC router and firewall will utilize a closed security policy. All services will be dropped, unless explicitly allowed. All services will be audited (drop or pass) on the firewall. This will ensure the most robust security stance, and allow containment of internet worms such as Code Red, and Nimbda.

NETWORK SECURITY ARCHITECTURE

Border Router

Cisco 3640, IOS v. 12.2, (1) 4 Serial Network Module, (2) Ethernet Network Modules

The Cisco 3640 will provide the border router function in the GIAC network architecture. It will be the first line of defense against external threats for the GIAC Enterprises network, due to its direct connection to the CloudNine internet ISP. This design will utilize the ability of the Cisco router to perform efficient static packet filtering, while providing a buffer against external threats for the perimeter firewall. The border router also serves as the last line of defense against outbound attacks originating from within the GIAC internal networks.

Selection of the Cisco 3640 met the following operational requirements:

Flexibility: The Cisco 3640 has several expansion slots, with a range of network adaptor cards available. This will allow GIAC Enterprises the option of adding internal network capacity, or upgrading to a higher capacity ISP internet connection as business requirements change.
Maintainability: Cisco is the most widely deployed router infrastructure in industry. There are extensive web resources available for Cisco router documentation, case studies, security guides, and configuration tools. Extensive local and web based training for Cisco routers, will ensure the availability of skilled Cisco support resources.

Maintainability: Cisco is the most widely deployed network routing infrastructure in industry. Deploying a Cisco router, will give GIAC access to an extensive support infrastructure and trained support staff.

Router Configuration Hardening

The Cisco 3640 will be configured to utilize only those services necessary. All other services will be shut off. Connections to the router will be allowed by exception. All other connections will be dropped. The National Security Agency, Router Security Configuration Guide, Report # C4-054R-00, 2001, will be used as a best practices guideline for securing the router.

Router Security Role

The Cisco 3640 router provides the primary perimeter network security mechanism. Placement at the GIAC network edge, allows leveraging the routers strong packet filtering capability to buffer the GIAC firewall and networks from external threats. The router provides the following network and security roles:

- Layer 3 static routing
- Ingress Filtering (ISP Interface)
    - Reserved IP Address
    - Multicast
    - Loopback
    - Anti-spoofing
    - Smurf

- Egress Filtering (ISP Interface)
- Packet Logging
- Defense in-depth layer 1 packet filtering for inbound external threats
- Defense in-depth layer 2 packet filtering for outbound internal threats

Firewall/VPN Appliance

Lucent Model 1000 Brick/VPN Appliance, LSMS v. 6.0.471

The Lucent Model 1000 Brick/VPN Appliance, will provide the second layer of defense against external threats, due to its deployment behind the border router. Its stateful packet filtering capability (including ip fragment reassembly) will be leveraged to enforce a ruleset on each physical firewall interface (virtual firewall), and provide two layers of ACL enforcement for all GIAC internal hosts. It also provides the first layer of defense against outbound attacks originating from within the GIAC internal networks.

The Brick 1000 will also provide the VPN tunnel capability for GIAC partners, suppliers, and remote employees. The respective VPN tunnels will be configured in the appropriate ruleset, to control access to the various GIAC IT resources. The VPN tunnel will be established via a Windows based Lucent IPSec 4.0.474 VPN client .

Selection of the Lucent Model 1000 Brick met the following operational requirements:

Flexibility: The Lucent Model 1000 Brick is a layer 2 firewall/vpn appliance. This allows the greatest flexibility with regards to network architecture design because a layer 2 device won't change the routing architecture (and network numbering), when it is deployed at difference locations within the internal networks. In addition, the Lucent Model 1000 Brick has 7 FastEthernet interfaces, and two Gigabit Ethernet interfaces, . This will give GIAC Enterprises a network upgrade migration path as business needs change.

Maintainability: The Lucent Model 1000 Brick administration interface is a secure web based interface. The firewall interface is an intuitive hierarchical application that is similar to the Windows explorer directory interface. All firewall rulesets, VPN's, and authentication can be administered via this interface, allowing GIAC to leverage the most functionality from a minimal support skillet.

Additional requirements met:

Efficient Disaster Recovery: The Lucent Model 1000 Brick appliance takes less than 5 minutes for a full OS and configuration reload (from a 3.5" floppy drive).

Denial of Service Management: The GIAC network architecture will utilize four denial of service management features of the Lucent Model 1000 Brick:

> Intelligent Cache Management(ICM)[1]: This feature allows the Lucent firewall appliance to efficiently manage memory during denial of service conditions. The firewall will prune

[1] See Lucent Security Management Server 6.0: Policy Guide, Appendix C-3, for a complete discussion of the Intelligent Cache Management feature.

sessions based on a user definable memory parameters (firewall memory threshold and floor), and a network traffic priority scheme. This priority scheme includes traffic classification based on protocol, and session auditing. The net affect of this feature is to minimize the impact of flooding type attacks against legitimate user traffic.

TCP Syn Flood Protection[2]: The Lucent Model 1000 Brick will be configured to use a rule based feature called TCP Syn Flood protection. The firewall will reset half-open TCP server connections based on user-defined criteria. The impact of this feature is to have the firewall close half-opened TCP connections to the GIAC servers, in order to prevent TCP SYN flooding denial of service conditions.

Destination Address Mapping[3]: The GIAC Enterprises network architecture will utilize destination address mapping for public services. This will enable GIAC Enterprises to do round-robin load balancing for all public services. Another benefit is that servers can be added or removed based on business (or maintenance) needs, without external user impact.

IP Fragment Re-assembly: The Lucent Model 1000 Brick does ip fragment reassembly. It checks for duplication and overlap, and discards invalid fragments.

Firewall Configuration Hardening

The Lucent Brick uses the Inferno operating system. The firewall OS kernel comes secure from the factory. It only includes those services necessary to communicate with the Lucent Security Management Server (these services are specified in the "firewall" and "administrative" brick zone rulesets). There are no services to turn on or off in the Brick Inferno operating system. The default Brick security policy ("firewall" zone ruleset), allows only encrypted connections between the firewall and the Lucent Security Management Server. The Brick will drop and log all other connection attempts against interfaces. Furthermore, the Solaris LSMS server used in the GIAC design is directly connected to the Brick and fully segmented from all hosts via the "AdministrativeZone" ruleset.

Firewall Security Role

The GIAC firewall provides the primary internal network access control mechanism. Centralizing the placement of the firewall between all internal network segments, allows the firewall to provide the highest access control granularity. Network security functions include:

[2] See Lucent Security Management Server 6.0: Policy Guide, Appendix C-1, for a complete discussion of the TCP Syn Flood feature.
[3] See Lucent Security Management Server 6.0: Policy Guide, 6-4, for a complete discussion of the destination address mapping feature.

- Stateful packet filtering
- Session auditing
- Defense in-depth layer 2 session filtering for external network threats
- Defense in-depth layers 1 & 2 session filtering for internal network threats.
- VPN access services (tunnel endpoint)
- Local authentication services
- Server ip address hiding and load balancing via destination address mapping
- DoS protection via SYN flood, and intelligent cache management mechanisms
- IP fragment management

GIAC ACCESS REQUIREMENT MATRIX

TYPE	ZONE	SVCS
General Internet	PubNet	dns, http, https, smtp
Network Management	All	syslog, ping, snmp
Data Transfer	PubNet, SecureNet, VpnNet	ssh
External Partner	VpnNet	VPN (https)
External Supplier	VpnNet	VPN (https)
Corporate Internet	GiacNet	ftp, http, https via proxy
External Corporate	GiacNet	VPN (all)

GIAC Enterprises

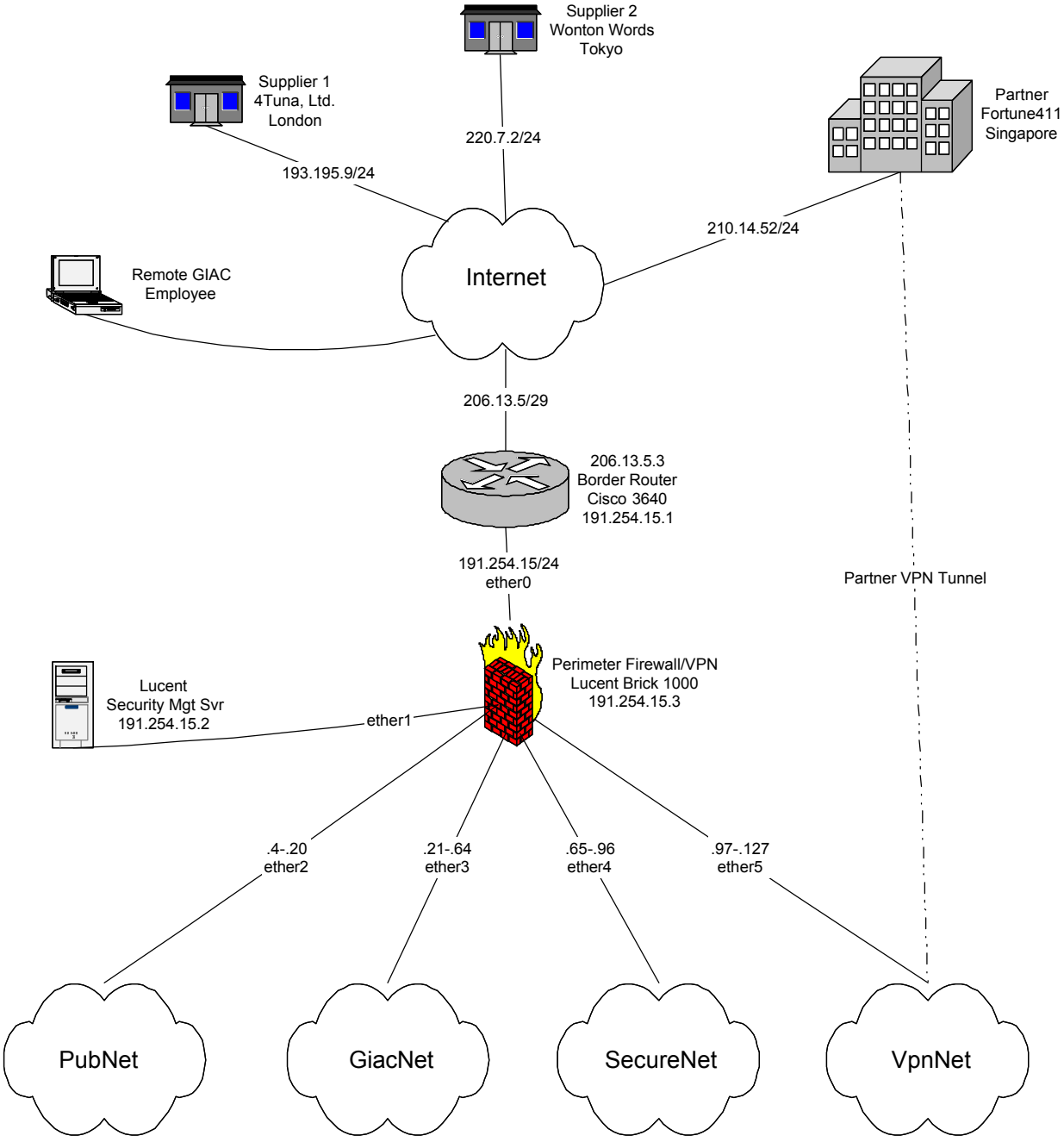


Figure 1

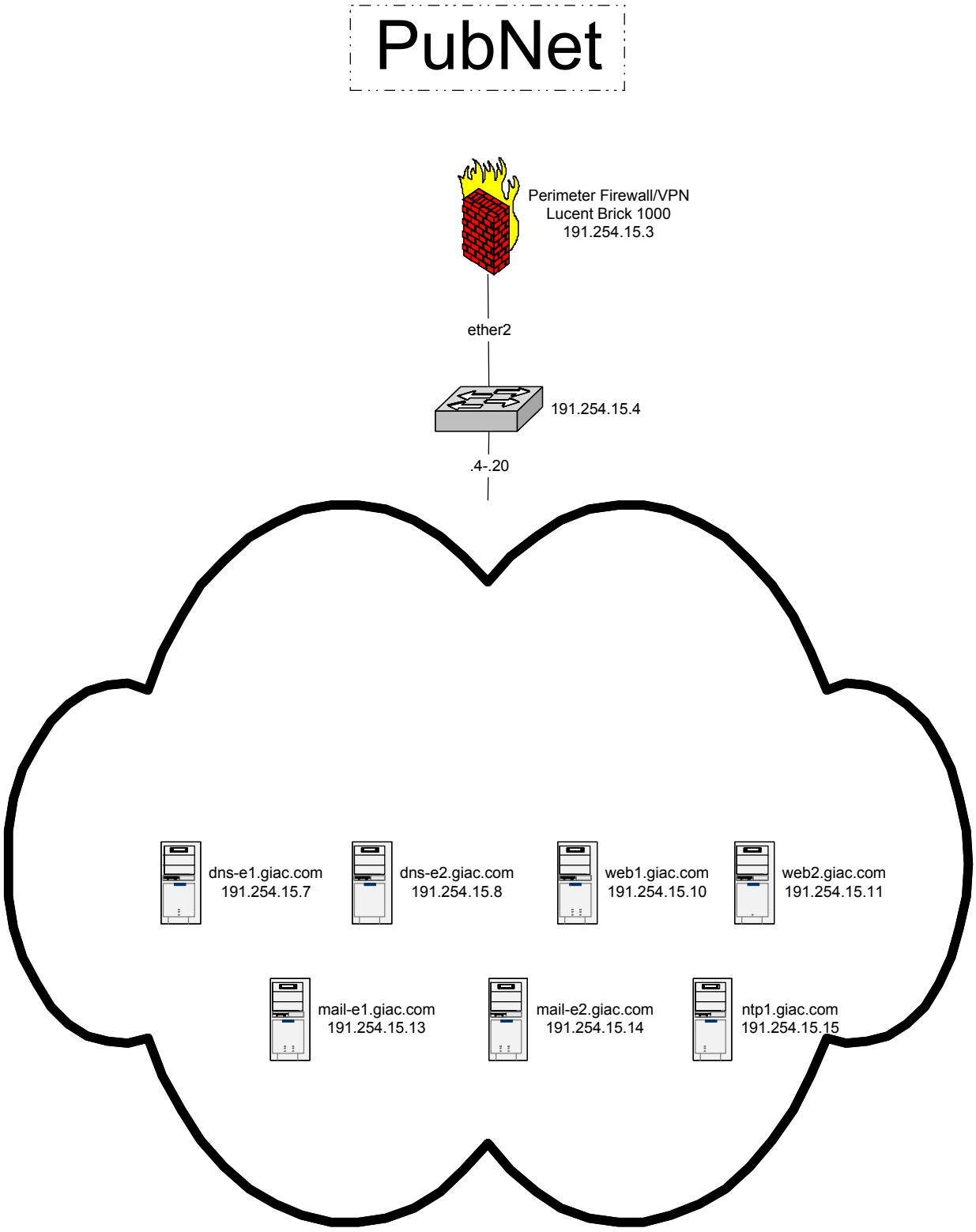


Figure 2

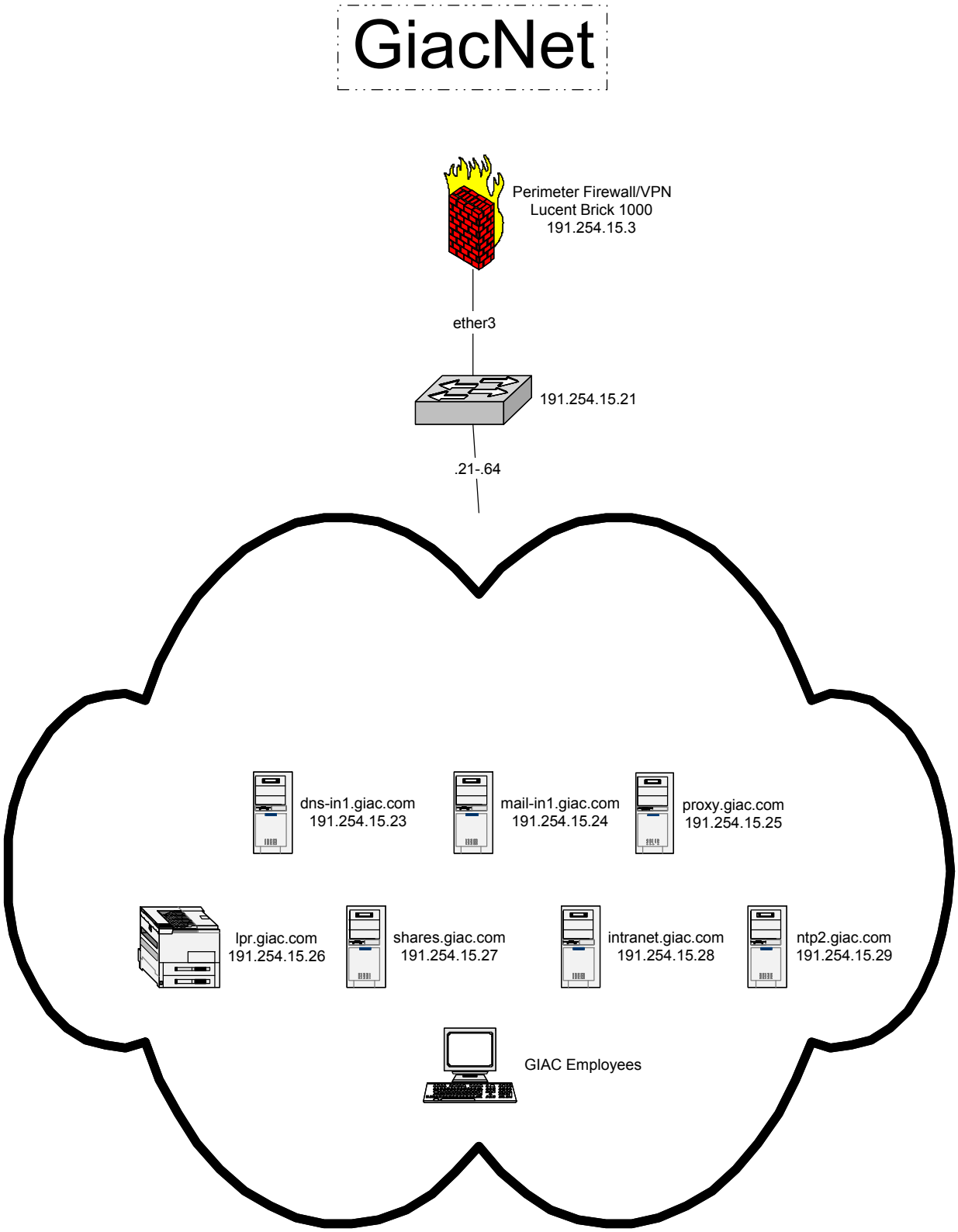


Figure 3

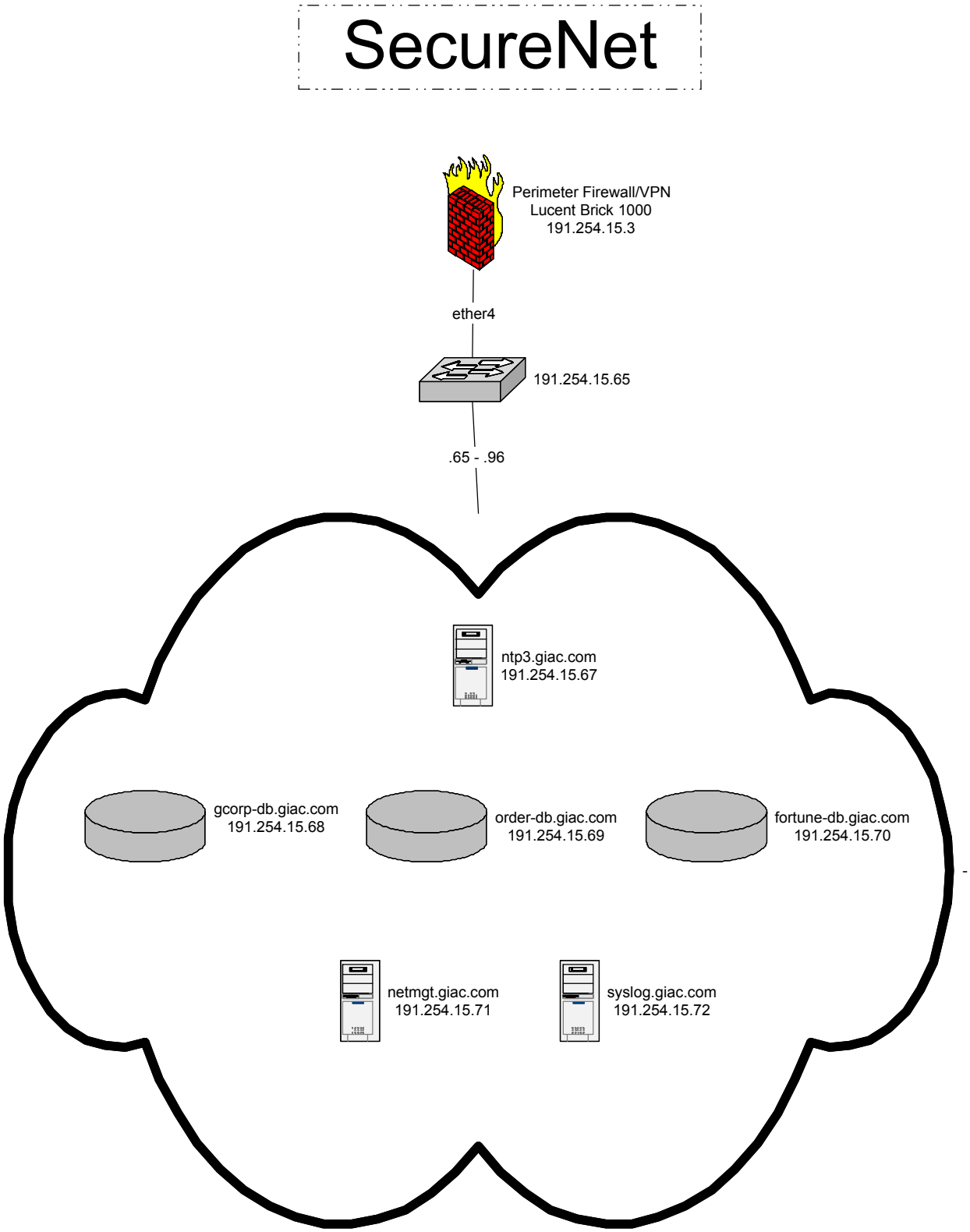

SecureNet
Perimeter Firewall/VPN
Lucent Brick 1000
191.254.15.3
ether4
191.254.15.65
.65 - .96
ntp3.giac.com
191.254.15.67
gcorp-db.giac.com
191.254.15.68
order-db.giac.com
191.254.15.69
fortune-db.giac.com
191.254.15.70
netmgt.giac.com
191.254.15.71
syslog.giac.com
191.254.15.72

Figure 4

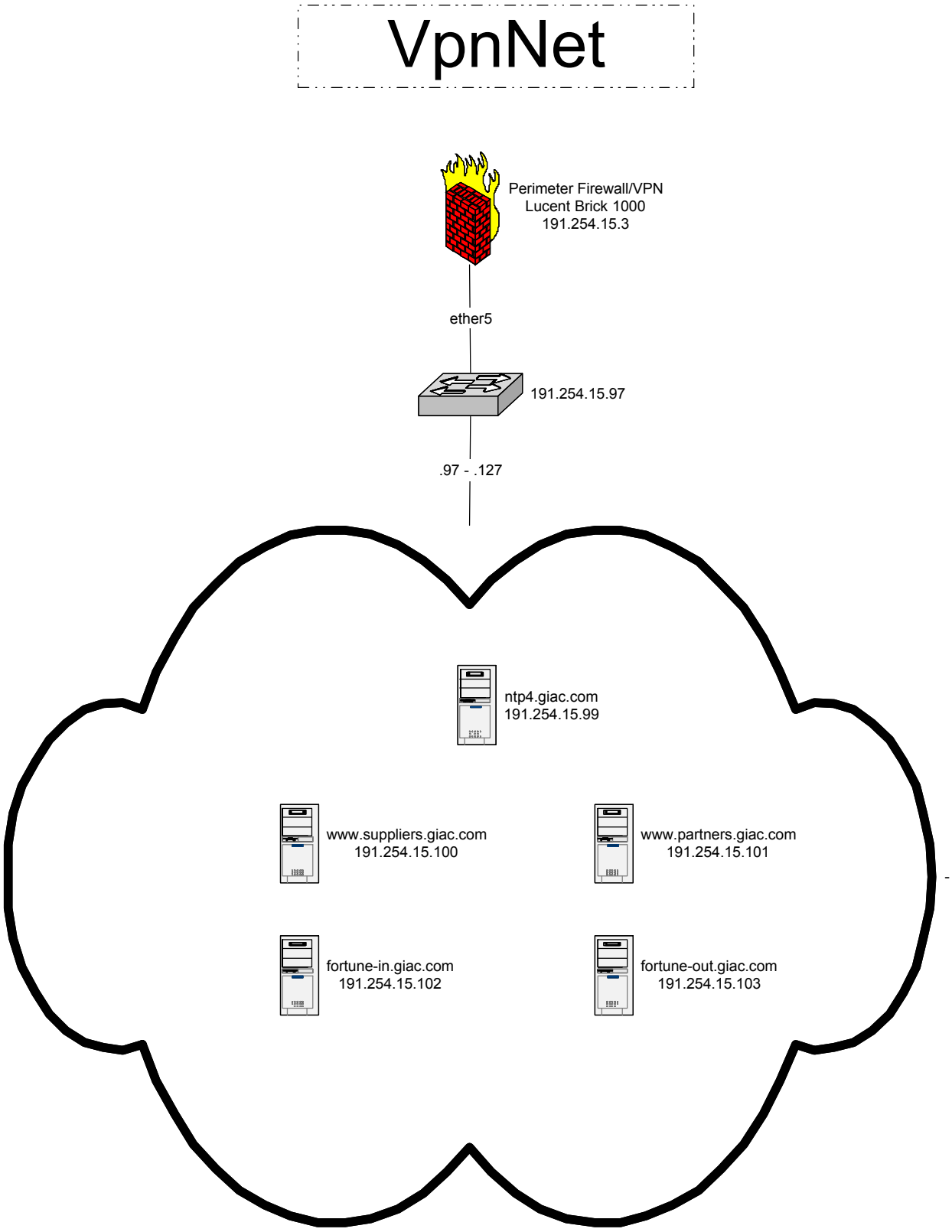


Figure 5

SECURITY POLICY

Border Router

```
!
version 12.2
!
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
! IOS Hardening
!
no cdp run
no boot network
no service config
no service tcp-small-servers
no service udp-small-servers
no ip finger
no ip http server
no ip bootp server
no ip source-route
!
logging on
logging server 191.254.15.72
!
hostname giac-router
!
enable secret 5 $1$PC5K$GsVRrXTVGYMo8CVq2Ih1
!
ip default-gateway  191.254.15.71
ip routing
ip subnet-zero
!
interface Ethernet 1/0
 description giac fw int 191.254.15.0/24
 ip address 191.254.15.1 255.255.255.0
 no ip directed-broadcast
 no ip mask-reply
 no ip redirects
 no ip proxy-arp
 no ip unreachable
 ip access-group 110 in
```

```
 ip access-group 111 out
!
interface Ethernet 2/0
 no description
 no ip address
 shutdown
!
interface Serial 0/0
 description CloudNine T1 Internet Connection
 ip address 206.13.5.3 255.255.255.248
 no ip directed-broadcast
 no ip mask-reply
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 encapsulation ppp
 bandwidth 1544
!
interface Serial 0/1
 no description
 no ip address
 shutdown
!
interface Serial 0/2
 no description
 no ip address
 shutdown
!
interface Serial 0/3
 no description
 no ip address
 shutdown
!
no router rip
!
banner motd /
```

This is a GIAC Enterprise computer system, which may be accessed and used only for authorized GIAC Enterprise business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with

confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.

```
/
!
ip classless
!
! VTY ACL
access-list 105 permit ip host 191.254.15.71 any
access-list 105 deny ip any any log
! SNMP ACL
access-list 106 permit udp host 191.254.15.71 any eq 161
access-list 106 deny ip any any log
! Ingress
! reserved ip / multicast / loopback / anti-spoofing / smurf
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 224.0.0.0 31.255.255.255 any log
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 191.254.15.0 0.0.0.255 any log
access-list 110 deny ip any host 191.254.15.0 log
access-list 110 deny ip any host 191.254.15.255 log
access-list 110 permit ip any any
! Egress
! PubNet VBA / GiacNet Proxy / GiacNet VBA / VpnNet VBA
access-list 111 permit ip host 191.254.15.6 any
access-list 111 permit ip host 191.254.15.25 any
access-list 111 permit ip host 191.254.15.30 any
access-list 111 permit ip host 191.254.15.104 any
access-list 111 deny ip any any log
! IP Static Routes
!
ip route 0.0.0.0 0.0.0.0 206.13.5.4
! SNMP Management
no snmp-server community public RO
no snmp-server admin RW
snmp-server community magoo RO 106
snmp-server location        GIAC HQ RM 428
snmp-server contact  GIAC N-OPS 7-2254
!
line console 0
 exec-timeout 0 0
 password 7 71C314107140004
```

```
 login
!
line vty 0 4
 session-timeout 10
 password 7 4040212030A272E1
 login
 ip access-group 105 in
!
ntp clock-period 17179931
ntp server 191.254.15.67 source eth 1/0
end
```

Primary Firewall

The following six brick zone rulesets are assigned to the GIAC firewall. The PubNet, GiacNet, SecureNet, and VpnNet rulesets are the custom rulesets generated from the GIAC business requirements. The remaining "administrativezone", and "firewall" rulesets are system generated to protect the LSMS server and the firewall itself. The brick zone assignment table is as follows:

GIAC Brick Zone Ruleset Assignments

Port	Zone Ruleset	Tunnel Endpoint / Virtual Brick Addr	Hosts Behind Tunnel / Zone IP Addresses
local	firewall@giac		*
ether0			*
ether1	administrativezone@giac		LSMS
ether2	pubnet	191.254.15.6	191.254.15.4-191.254.15.20
ether3	giacnet	191.254.15.30	191.254.15.21-191.254.15.64
ether4	securenet	191.254.15.73	191.54.15.65-191.254.15.96
ether5	vpnnet	191.254.15.104	191.254.15.97-191.254.15.127

GIAC Custom Brick Zone Rulesets

Ruleset: PubNet

RULES - BASIC

Active	Rule No.	Description	Direction	Source	Destination	Service	Action	Audit Session
yes	1000	PASS IB DNS	in	*	pubnet-vba	dns	pass	basic
yes	1001	PASS IB EXTERNAL HTTP	in	*	pubnet-vba	http	pass	basic
yes	1002	PASS IB EXTERNAL HTTPS	in	*	pubnet-vba	https	pass	basic
yes	1003	PASS IB EXTERNAL SMTP	in	*	pubnet-vba	smtp	pass	basic
yes	1004	PASS IB INTERNAL SMTP TO EXTERNAL GATEWAYS	in	mail-in1.giac.com	mail.giac.com	smtp	pass	basic
yes	1005	PASS IB ping_request from GIAC NET MGT SVR	in	netmgt.giac.com	*	ping_request	pass	basic
yes	1006	PASS IB ping_request from GIAC NET MGT SVR	in	netmgt.giac.com	*	snmp	pass	basic
yes	1007	PASS IB from order-db to www	in	order-db.giac.com	www.giac.com	ssh	pass	basic
yes	1008	PASS OB DNS REQUESTS	out	dns.giac.com	*	dns	pass	basic
yes	1009	PASS OB SMTP	out	mail.giac.com	*	smtp	pass	basic
yes	1010	PASS OB SYSLOG TO syslog.giac.com	out	*	syslog.giac.com	syslog	pass	basic
yes	65535	drop all traffic that does not match any rule	both	*	*	*	drop	basic

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	1000						true	300	none	timeout_reset	3	1000
yes	1001						true	300	none	timeout_reset	3	1000
yes	1002						true	300	none	timeout_reset	3	1000
yes	1003						true	300	none	timeout_reset	3	1000
yes	1004						true	300	none	none		
yes	1005						true	10	none	none		
yes	1006						true	30	none	none		
yes	1007						true	300	none	none		
yes	1008						true	300	none	none		
yes	1009						true	10	none	none		
yes	1010						true	30	none	none		
yes	65535						true	10	none	none		

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	1000		pool	dns.giac.com	pool	
yes	1001		pool	www.giac.com	pool	
yes	1002		pool	www.giac.com	pool	
yes	1003		pool	mail.giac.com	pool	
yes	1004		pool		pool	
yes	1005		pool		pool	

yes	1006		pool		pool	
yes	1007		pool		pool	

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	1008		pool		pool	
yes	1009		pool		pool	
yes	1010		pool		pool	
yes	65535					

DEPENDENCY MASKS

Name	Description	Source IP	Destination IP	Service	Action	Authenticated	Alarm Code	Hit Count

SERVICE GROUPS

Name	Description	Proto/Dst Port/Src Port	Application-Layer Monitoring
dns	domain name system service (TCP)	tcp/53/*	none
dns	domain name system service (TCP)	udp/53/*	none
http	hyper text service	tcp/80/*	none
https	secure hyper text service	tcp/443/*	none
ping_request	ping service	icmp/8/0	none
smtp	SMTP	tcp/25/*	none
snmp	SNMP Request	udp/161/*	none
ssh	Secure shell	tcp/22/*	none
syslog	Syslog	udp/514/*	none

HOST GROUPS

Name	Description	Address or Range
dns.giac.com	DNS SVR POOL	191.254.15.7
dns.giac.com	DNS SVR POOL	191.254.15.8
mail-in1.giac.com	GIAC INTERNAL SMTP SVR1	191.254.15.24
mail.giac.com	SMTP SVR POOL	191.254.15.13
mail.giac.com	SMTP SVR POOL	191.254.15.14
netmgt.giac.com	NETWORK MGT SVR	191.254.15.71
order-db.giac.com	ORDER DB	191.254.15.69
pubnet-vba	PubNet Virtual Brick Address -- DST ADDRESS MAPPING	191.254.15.6
syslog.giac.com	SYSLOG SVR	191.254.15.72
www.giac.com	WWW SVR POOL	191.254.15.10
www.giac.com	WWW SVR POOL	191.254.15.11

Ruleset: GiacNet

RULES - BASIC

Active	Rule No.	Description	Direction	Source	Destination	Service	Action	Audit Session
yes	305	proxy requests from VPN users for SW upgrade	in	~Active_VPN_Users	Virtual Brick Address	6/443/*	vpn proxy	basic
yes	306	proxy requests from VPN users for SW upgrade	out	~Active_VPN_Users	Virtual Brick Address	6/443/*	vpn proxy	basic
yes	310	proxy user authentication requests	both	*	Virtual Brick Address	6/443/*	proxy	basic
yes	410	allow anyone outside to initiate IKE to this TEP (VPN Internal case)	out	*	Virtual Brick Address	udp/500/*	pass	basic
yes	411	allow us to initiate IKE from this TEP (VPN Internal case)	in	Virtual Brick Address	*	udp/500/500	pass	basic
yes	412	allow us to send client/far end session maintenance messages (VPN Internal case)	in	Virtual Brick Address	~Active_VPN_UserTEPs	udp/*/500	pass	basic
yes	420	allow anyone outside to initiate IKE to this TEP (VPN External case)	in	*	Virtual Brick Address	udp/500/*	pass	basic
yes	430	allow tunnels to be decrypted (VPN External case)	in	*	Virtual Brick Address	ipsec	vpn	basic
yes	440	allow tunnels to be decrypted (VPN Internal case)	out	*	Virtual Brick Address	ipsec	vpn	basic
yes	1000	PASS IB ping_request from netmgt.giac.com	in	netmgt.giac.com	*	ping_request	pass	basic
yes	1001	PASS IB SNMP from netmgt.giac.com	in	netmgt.giac.com	*	snmp	pass	basic
yes	1002	PASS IB VPN remote users -- local authentication	in	remote-users	*	*	vpn	basic
yes	1003	PASS OB securenet-vba VPN	out	*	securenet-vba	UDP_Encapsulation_Ports	pass	basic
yes	1004	PASS OB FTP PROXY	out	proxy.giac.com	*	ftp	pass	basic
yes	1005	PASS OB SECURE HTTP PROXY	out	proxy.giac.com	*	https	pass	basic
yes	1006	PASS OB WEB PROXY	out	proxy.giac.com	*	http	pass	basic
yes	1007	PASS OB SMTP TO EXTERNAL GATEWAYS	out	mail-in1.giac.com	mail.giac.com	smtp	pass	basic
yes	1008	PASS OB SYSLOG to syslog.giac.com	out	*	syslog.giac.com	syslog	pass	basic
yes	65535	drop all traffic that does not match any rule	both	*	*	*	drop	basic

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	305		30			external	true	300	none	none		
yes	306		30			external	true	300	none	none		
yes	310		30				true	300	none	none		
yes	410						true	300	none	none		
yes	411						true	300	none	none		
yes	412						true	120	none	none		
yes	420						true	300	none	none		
yes	430					external	true	300	none	none		
yes	440					internal	true	300	none	none		
yes	1000						true	10	none	none		
yes	1001						true	30	none	none		
yes	1002					external	true	300	none	none		
yes	1003						true	300	none	none		
yes	1004						true	300	none	none		
yes	1005						true	300	none	none		
yes	1006						true	300	none	none		
yes	1007						true	300	none	none		
yes	1008						true	30	none	none		

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	65535						true	10	none	none		

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	305		pool		pool	
yes	306		pool		pool	
yes	310		pool		pool	
yes	410					
yes	411					
yes	412					
yes	420					
yes	430					
yes	440					
yes	1000		pool		pool	
yes	1001		pool		pool	
yes	1002		pool		pool	
yes	1003		pool		pool	
yes	1004		pool		pool	
yes	1005		pool		pool	
yes	1006		pool		pool	
yes	1007		pool		pool	
yes	1008		pool		pool	
yes	65535					

DEPENDENCY MASKS

Name	Description	Source IP	Destination IP	Service	Action	Authenticated	Alarm Code	Hit Count

SERVICE GROUPS

Name	Description	Proto/Dst Port/Src Port	Application-Layer Monitoring
ftp	ftp service	tcp/21/*	none
http	hyper text service	tcp/80/*	none
https	secure hyper text service	tcp/443/*	none
ipsec	IPSEC (ESP only)	50/*/*	none
ipsec	IPSEC (ESP only)	51/*/*	none
ping_request	ping service	icmp/8/0	none

SERVICE GROUPS

Name	Description	Proto/Dst Port/Src Port	Application-Layer Monitoring
smtp	SMTP	tcp/25/*	none
snmp	SNMP Request	udp/161/*	none
syslog	Syslog	udp/514/*	none

HOST GROUPS

Name	Description	Address or Range
mail-in1.giac.com	GIAC INTERNAL SMTP SVR1	191.254.15.24
mail.giac.com	SMTP SVR POOL	191.254.15.13
mail.giac.com	SMTP SVR POOL	191.254.15.14
netmgt.giac.com	NETWORK MGT SVR	191.254.15.71
proxy.giac.com	GIAC WEB PROXY SVR	191.254.15.25
securenet-vba	SecureNet -- Virtual Brick Address	191.254.15.73
syslog.giac.com	SYSLOG SVR	191.254.15.72

Ruleset: SecureNet

RULES - BASIC

Active	Rule No.	Description	Direction	Source	Destination	Service	Action	Audit Session
yes	305	proxy requests from VPN users for SW upgrade	in	~Active_VPN_Users	Virtual Brick Address	6/80/*	vpn proxy	basic
yes	306	proxy requests from VPN users for SW upgrade	out	~Active_VPN_Users	Virtual Brick Address	6/80/*	vpn proxy	basic
yes	310	proxy user authentication requests	both	*	Virtual Brick Address	6/80/*	proxy	basic

yes	410	allow anyone outside to initiate IKE to this TEP (VPN Internal case)	out	*	Virtual Brick Address	udp/500/*	pass	basic
yes	411	allow us to initiate IKE from this TEP (VPN Internal case)	in	Virtual Brick Address	*	udp/500/500	pass	basic
yes	412	allow us to send client/far end session maintenance messages (VPN Internal case)	in	Virtual Brick Address	~Active_VPN_UserTEPs	udp/*/500	pass	basic
yes	420	allow anyone outside to initiate IKE to this TEP (VPN External case)	in	*	Virtual Brick Address	udp/500/*	pass	basic
yes	430	allow tunnels to be decrypted (VPN External case)	in	*	Virtual Brick Address	ipsec	vpn	basic
yes	440	allow tunnels to be decrypted (VPN Internal case)	out	*	Virtual Brick Address	ipsec	vpn	basic
yes	1000	PASS IB syslog from giac-nw-range to syslog.giac.com	in	giac-nw-range	syslog.giac.com	syslog	pass	basic
yes	1001	PASS IB hr-db VPN to gcorp-db	in	hr	gcorp-db.giac.com	hr-db	vpn	basic
yes	1002	PASS OB ping_request from netmgt.giac.com to giac-nw-range	out	netmgt.giac.com	giac-nw-range	ping_request	pass	basic
yes	1003	PASS OB SNMP from netmgt.giac.com to giac-nw-range	out	netmgt.giac.com	giac-nw-range	snmp	pass	basic
yes	1004	PASS OB SSH from fortune-db.giac.com to fortune-out.giac.com	out	fortune-db.giac.com	fortune-out.giac.com	ssh	pass	basic
yes	1005	PASS OB SSH from fortune-db.giac.com to fortune-in.giac.com	out	fortune-db.giac.com	fortune-in.giac.com	ssh	pass	basic
yes	1006	PASS OB SSH from order-db-giac.com to www.giac.com	out	order-db.giac.com	www.giac.com	ssh	pass	basic
yes	65535	drop all traffic that does not match any rule	both	*	*	*	drop	basic

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	305		30			external	true	300	none	none		
yes	306		30			external	true	300	none	none		
yes	310		30				true	300	none	none		
yes	410						true	300	none	none		
yes	411						true	300	none	none		
yes	412						true	120	none	none		
yes	420						true	300	none	none		
yes	430					external	true	300	none	none		
yes	440					internal	true	300	none	none		
yes	1000						true	30	none	none		
yes	1001					external	true	300	none	none		
yes	1002						true	10	none	none		
yes	1003						true	30	none	none		
yes	1004						true	300	none	none		
yes	1005						true	300	none	none		
yes	1006						true	300	none	none		
yes	65535						true	10	none	none		

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	305					
yes	306					
yes	310					
yes	410					
yes	411					
yes	412					
yes	420					
yes	430					
yes	440					
yes	1000		pool		pool	
yes	1001		pool		pool	
yes	1002		pool		pool	
yes	1003		pool		pool	
yes	1004		pool		pool	
yes	1005		pool		pool	
yes	1006		pool		pool	
yes	65535					

SERVICE GROUPS

Name	Description	Proto/Dst Port/Src Port	Application-Layer Monitoring
hr-db	Human Resources DB	tcp/1654/*	SQL*Net
ipsec	IPSEC (ESP only)	50/*/*	none
ipsec	IPSEC (ESP only)	51/*/*	none
ping_request	ping service	icmp/8/0	none
snmp	SNMP Request	udp/161/*	none
ssh	Secure shell	tcp/22/*	none
syslog	Syslog	udp/514/*	none

HOST GROUPS

Name	Description	Address or Range
fortune-db.giac.com	ALL THE FORTUNES -- BABY!	191.254.15.70
fortune-in.giac.com	INBOUND SUPPLIER FORTUNE SVR	191.254.15.102
fortune-out.giac.com	OUTBOUND PARTNER FORTUNE SVR	191.254.15.103
gcorp-db.giac.com	CORP DB -- HR .. PAYROLL	191.254.15.68
giac-nw-range	GIAC Network Range	191.254.15.1-191.254.15.255

HOST GROUPS

Name	Description	Address or Range
netmgt.giac.com	NETWORK MGT SVR	191.254.15.71
order-db.giac.com	ORDER DB	191.254.15.69
syslog.giac.com	SYSLOG SVR	191.254.15.72
www.giac.com	WWW SVR POOL	191.254.15.10

www.giac.com	WWW SVR POOL	191.254.15.11

Ruleset: VpnNet

RULES - BASIC

Active	Rule No.	Description	Direction	Source	Destination	Service	Action	Audit Session
yes	100	Perform UDP Decapsulation	in	*	Virtual Brick Address	UDP_Encapsulation_Ports	pass	basic
yes	101	Perform UDP Decapsulation	out	Virtual Brick Address	*	UDP_Encapsulation_Ports	pass	basic
yes	102	Perform UDP Decapsulation	in	Virtual Brick Address	*	UDP_Encapsulation_Ports	pass	basic
yes	103	Perform UDP Decapsulation	out	*	Virtual Brick Address	UDP_Encapsulation_Ports	pass	basic
yes	305	proxy requests from VPN users for SW upgrade	in	~Active_VPN_Users	Virtual Brick Address	6/443/*	vpn proxy	basic
yes	306	proxy requests from VPN users for SW upgrade	out	~Active_VPN_Users	Virtual Brick Address	6/443/*	vpn proxy	basic
yes	310	proxy user authentication requests	both	*	Virtual Brick Address	6/443/*	proxy	basic
yes	410	allow anyone outside to initiate IKE to this TEP (VPN Internal case)	out	*	Virtual Brick Address	udp/500/*	pass	basic
yes	411	allow us to initiate IKE from this TEP (VPN Internal case)	in	Virtual Brick Address	*	udp/500/500	pass	basic
yes	412	allow us to send client/far end session maintenance messages (VPN Internal case)	in	Virtual Brick Address	~Active_VPN_UserTEPs	udp/*/500	pass	basic
yes	420	allow anyone outside to initiate IKE to this TEP (VPN External case)	in	*	Virtual Brick Address	udp/500/*	pass	basic
yes	430	allow tunnels to be decrypted (VPN External case)	in	*	Virtual Brick Address	ipsec	vpn	basic
yes	440	allow tunnels to be decrypted (VPN Internal case)	out	*	Virtual Brick Address	ipsec	vpn	basic
yes	1000	PASS IB VPN from partners to www.partners.giac.com	in	partners	www.partners.giac.com	https	vpn	basic
yes	1001	PASS IB VPN from suppliers to www.suppliers.giac.com	in	suppliers	www.suppliers.giac.com	https	vpn	basic
yes	1002	PASS IB ping_request from netmgt.giac.com	in	netmgt.giac.com	*	ping_request	pass	basic
yes	1003	PASS IB SNMP to netmgt.giac.com	in	netmgt.giac.com	*	snmp	pass	basic
yes	1004	PASS IB SSH from fortune-db to fortune-out	in	fortune-db.giac.com	fortune-out.giac.com	ssh	pass	basic

yes	1005	PASS IB SSH from fortune-db to fortune-in	in	fortune-db.giac.com	fortune-in.giac.com	ssh	pass	basic
yes	1006	PASS OB syslog to syslog.giac.com	out	*	syslog.giac.com	syslog	pass	basic
yes	65535	drop all traffic that does not match any rule	both	*	*	*	drop	basic

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	100						true	300	none	none		
yes	101						true	300	none	none		
yes	102						true	300	none	none		
yes	103						true	300	none	none		
yes	305		30			external	true	300	none	none		
yes	306		30			external	true	300	none	none		
yes	310		30				true	300	none	none		
yes	410						true	300	none	none		
yes	411						true	300	none	none		
yes	412						true	120	none	none		
yes	420						true	300	none	none		
yes	430					external	true	300	none	none		
yes	440					internal	true	300	none	none		
yes	1000					external	true	300	none	timeout_reset	3	1000
yes	1001					external	true	300	none	timeout_reset	3	1000
yes	1002						true	10	none	none		

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	1003						true	30	none	none		
yes	1004						true	300	none	none		
yes	1005						true	300	none	none		
yes	1006						true	30	none	none		
yes	65535						true	10	none	none		

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	100		pool		pool	
yes	101		pool		pool	
yes	102		pool		pool	
yes	103		pool		pool	
yes	305		pool		pool	
yes	306		pool		pool	
yes	310		pool		pool	
yes	410					
yes	411					

yes	412					
yes	420					
yes	430					
yes	440					
yes	1000		pool		pool	
yes	1001		pool		pool	
yes	1002		pool		pool	
yes	1003		pool		pool	
yes	1004		pool		pool	
yes	1005		pool		pool	
yes	1006		pool		pool	
yes	65535					

SERVICE GROUPS

Name	Description	Proto/Dst Port/Src Port	Application-Layer Monitoring
https	secure hyper text service	tcp/443/*	none
ipsec	IPSEC (ESP only)	50/*/*	none
ipsec	IPSEC (ESP only)	51/*/*	none
ping_request	ping service	icmp/8/0	none
snmp	SNMP Request	udp/161/*	none
ssh	Secure shell	tcp/22/*	none
syslog	Syslog	udp/514/*	none

HOST GROUPS

Name	Description	Address or Range
fortune-db.giac.com	ALL THE FORTUNES -- BABY!	191.254.15.70
fortune-in.giac.com	INBOUND SUPPLIER FORTUNE SVR	191.254.15.102
fortune-out.giac.com	OUTBOUND PARTNER FORTUNE SVR	191.254.15.103
netmgt.giac.com	NETWORK MGT SVR	191.254.15.71
partners	GIAC Partner Network Ranges	210.14.52.2-210.14.52.254
suppliers	GIAC Supplier Network Ranges	193.195.9.2-193.195.9.254
suppliers	GIAC Supplier Network Ranges	220.7.2.2-220.7.2.254
syslog.giac.com	SYSLOG SVR	191.254.15.72
www.partners.giac.com	PARTNERS WEB SVR	191.254.15.101
www.suppliers.giac.com	SUPPLIERS WEB SVR	191.254.15.100

System Rulesets

The next two rulesets (firewall@giac, administrativezone@giac), are generated by the LSMS application when creating the giac-spf1 firewall instance. The "firewall@giac" zone ruleset is automatically generated by the LSMS application and applied to all firewall interfaces (local). It's job is to protect the firewall, and only allow communications between the firewall, and the LSMS server. The administrativezone@giac zone ruleset job is to protect the LSMS firewall administration server. This zone must be manually applied to the firewall interface that the LSMS server is attached to.

Ruleset: firewall@giac

RULES - BASIC

Active	Rule No.	Description	Direction	Source	Destination	Service	Action	Audit Session
yes	200	allow brick to open sessions to the LSMS	out	*	LSMS	*	pass	basic
yes	201	allow LSMS to open sessions to the brick	in	LSMS	*	brick_from_SMS_Services	pass	basic
yes	202	allow ICMP Communication Prohibited messages to be sent for Drop+Notify action	out	*	*	1/3/13	pass	basic
yes	203	allow VPN control packets into firewall	in	*	*	udp/500/*	pass	basic
yes	204	allow VPN control packets from firewall to client	out	*	*	udp/*/500	pass	basic
yes	205	allow Reflection packets from proxy/LSMS to firewall	in	*	*	udp/1024/*	pass	basic
yes	65535	drop all traffic that does not match any rule	both	*	*	*	drop	basic

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	200						true	300	none	none		
yes	201						true	300	none	none		
yes	202						true	300	none	none		
yes	203						true	59	none	none		
yes	204						true	59	none	none		
yes	205						true	300	none	none		
yes	65535						true	10	none	none		

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	200					
yes	201					
yes	202					
yes	203					
yes	204					
yes	205					
yes	65535					

SERVICE GROUPS			
Name	**Description**	**Proto/Dst Port/Src Port**	**Application-Layer Monitoring**
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	tcp/910/*	none
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	icmp/8/0	none
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	udp/1024/*	none
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	udp/9014/*	none

HOST GROUPS		
Name	**Description**	**Address or Range**
LSMS		137.187.152.126

Ruleset: administrativezone@giac

RULES - BASIC

Active	Rule No.	Description	Direction	Source	Destination	Service	Action	Audit Session
yes	200	allow bricks to send audit data to the LSMS and request downloads	in	brickRemoteAddresses	LSMS	brick_to_SMS_Services	pass	basic
yes	201	allow LSMS to download policy and configuration information to bricks	out	LSMS	brickLocalAddresses	brick_from_SMS_Services	pass	basic
yes	202	allow policy download replies from brick to LSMS when Clear Cache option is used	in	brickRemoteAddresses	LSMS	tcp/*/910	pass	none
yes	203	allow bricks to send audit data to the LSMS and request downloads	in	*	LSMS	brick_to_SMS_Services	pass	basic
yes	204	allow LSMS to download policy and configuration information to bricks	out	LSMS	*	brick_from_SMS_Services	pass	basic
yes	205	allow policy download replies from brick to LSMS when Clear Cache option is used	in	*	LSMS	tcp/*/910	pass	none
yes	320	allow user authentication requests to be reflected from brick VBAs to the LSMS	in	Bricks_VBA	LSMS	userAuth	pass	basic
yes	65535	drop all traffic that does not match any rule	both	*	*	*	drop	basic

RULES - ADVANCED

Active	Rule No.	Max Use Total	Max Use Concurrent	Alarm Code	Dependency Mask	Virtual Private Network	Authorize Return Channel	Session Timeout	Drop Action	Syn Flood Type	Syn Flood Timeout	Syn Flood Threshold
yes	200						true	300	none	none		
yes	201						true	300	none	none		
yes	202						true	300	none	none		
yes	203						true	300	none	none		
yes	204						true	300	none	none		
yes	205						true	300	none	none		
yes	320						true	300	none	none		
yes	65535						true	10	none	none		

RULES - ADDRESS TRANSLATION

Active	Rule No.	Source Address Mapping	Source Address Mapping Type	Destination Address Mapping	Destination Address Mapping Type	Destination Port Mapping
yes	200	brickLocalAddresses	direct			
yes	201			brickRemoteAddresses	direct	
yes	202	brickLocalAddresses	direct			
yes	203					
yes	204					
yes	205					
yes	320					
yes	65535					

SERVICE GROUPS

Name	Description	Proto/Dst Port/Src Port	Application-Layer Monitoring
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	tcp/910/*	none
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	icmp/8/0	none
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	udp/1024/*	none
brick_from_SMS_Services	service group (brick<-LSMS) for managing bricks	udp/9014/*	none
brick_to_SMS_Services	service group (brick->LSMS) for managing bricks	tcp/900/*	none
brick_to_SMS_Services	service group (brick->LSMS) for managing bricks	tcp/9000-9001/*	none
brick_to_SMS_Services	service group (brick->LSMS) for managing bricks	udp/9014/*	none

userAuth	VBA to SMS for user authentication	tcp/9010-9011/*	none

HOST GROUPS		
Name	**Description**	**Address or Range**
Bricks_VBA		191.254.15.6
Bricks_VBA		191.254.15.104
Bricks_VBA		191.254.15.30
Bricks_VBA		191.254.15.73
LSMS		137.187.152.126

Policy Tutorial

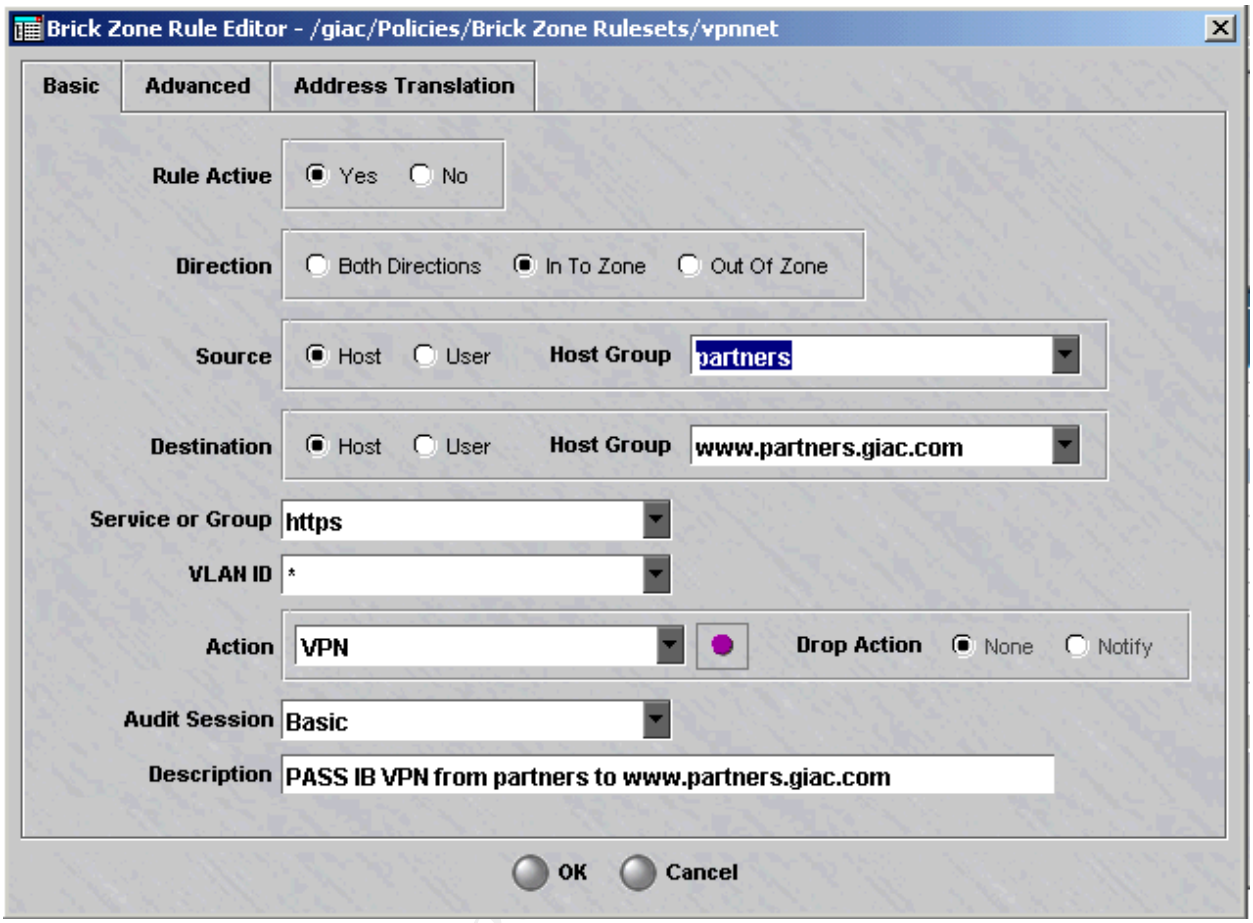
The Lucent Brick is a layer 2 network device that uses brick zone rulesets to encapsulate the network security rules. Each zone is a collection of rules that act as virtual firewall to the interface on which it is applied. The Lucent Brick can have many zones applied to one firewall interface, or one zone applied across many firewalls and/or interfaces.

Each firewall rule may also reference host groups and service groups in order to simplify security rule maintenance. The firewall administrator can generate custom host groups and service groups according to the security requirements of the organization, or use the default service groups that come pre-configured with the Lucent firewall application.

Rule Syntax and Attributes

Firewall administrator use the "Brick Zone Rule Editor" from the LSMS Remote Navigator application to create and manage firewall rules. There are three tabs (Basic, Advanced, Address Translation), that control the rule configuration. The following sections describe each rule configuration tab using Rule 1000 of the VpnNet ruleset.

Rule Attributes -- Basic

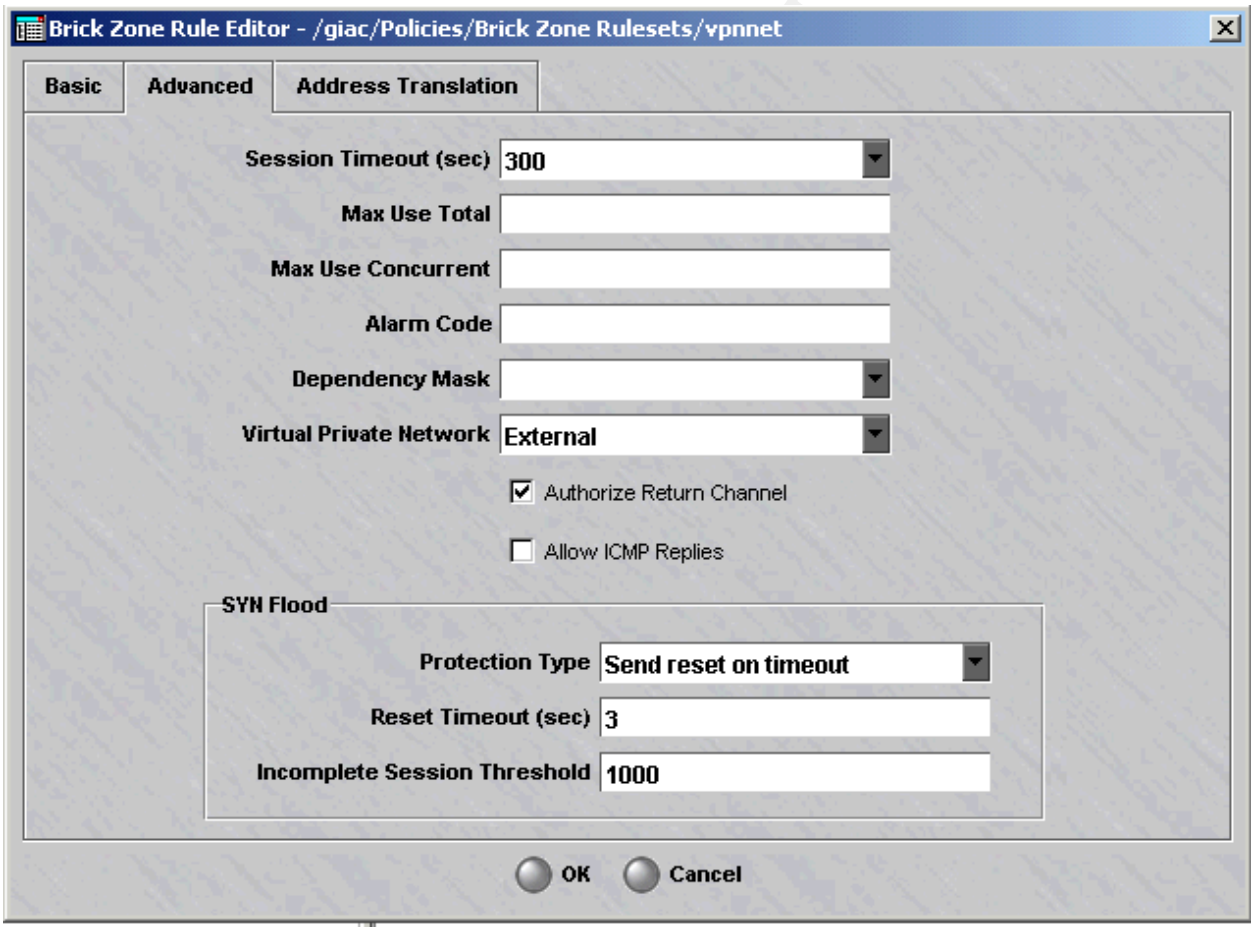


Basic Rule Attribute	Description
Rule Active [yes | no]	Turn rule on or off
Direction [both | in | out]	Specify direction to apply rule. "both" means either direction. "in" means out of the firewall interface. "out" means into the firewall interface.

Source [Host | User]	"Host" specifies host group. A host group is a set of IP addresses. It can be a single ip address, a range of ip addresses, or the wildcard address (*) meaning any ip address. Host groups are referenced via their name, and deliniate each ip address belonging to the group. the source ip address of the session originator. This can be a numeric ip address, host group, or any address (*). If set to "User", firewall verifies identity of session originator via user group based authentication.
Destination [Host | User]	"Host" specifies the destination ip address delineated by the session originator. This can be a numeric ip address, host group, or any address (*). If set to "User", firewall verifies identity of session originator via user group based authentication.
Service or Group	The service group specifies the service, including protocol, destination port, and/or source port. Each service attribute can also contain the wildcard (*) character, meaning that the service group applies to any protocol/destination port/source port.
VLAN ID [VLAN #]	Virtual LAN number. Lucent firewalls can be configured to apply rulesets based on 802.1Q VLAN tags.
Action [Drop | Pass | Proxy | VPN | VPN Proxy]	"Drop" means discard sessions not matching rule. "Pass" means to forward sessions matching rule. "Proxy" means to forward (reflect via NAT) sessions to a host running the Lucent Proxy Agent (LPA), for application level inspection. Lucent LSMS 6..471 currently supports proxying of the smtp, and http protocols. "VPN" means firewall encrypts or decrypts session traffic. "VPN Proxy" means firewall encrypt or decrypts session, and then forwards sessions (via NAT) to LPA proxy host.

Audit Session [Basic | Detailed]	"Basic" means log all open and closed session packets (both dropped and passed sessions). "Detailed" means "Basic" auditing plus application layer logging for the following protocols – TFTP, FTP, H.323, SQL*Net, or NetBIOS .
Description	Optional rule description.

Rule Attributes – Advanced

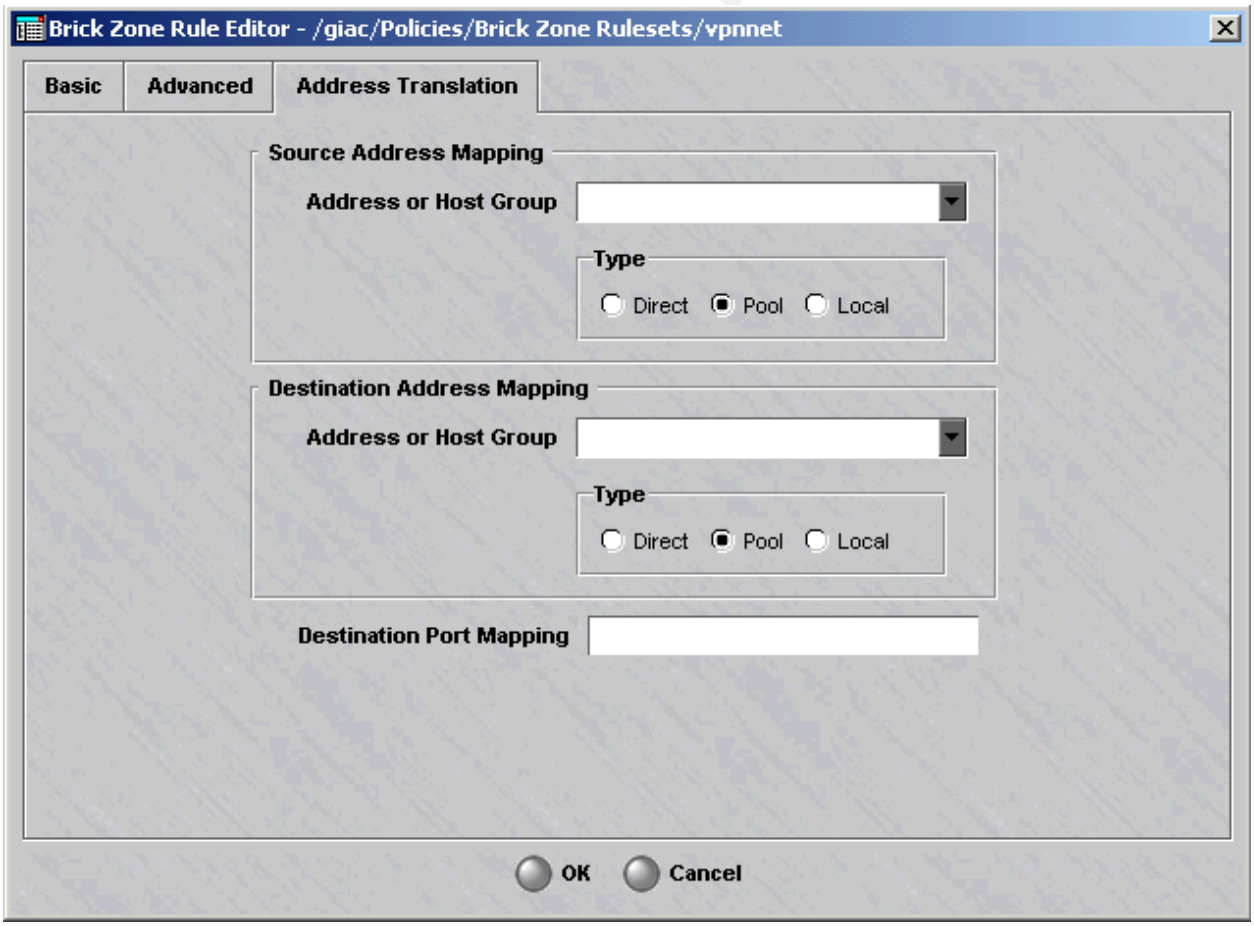


Rule Attributes – Address Translation

Advanced Rule Attribute	Description

Session Timeout [seconds]	Period of time a session entry remains in the firewall session cache. Default session timeouts for rule with "Pass" action are: TCP = 300 seconds, UDP = 30 seconds, ICMP = 10 seconds
Max Use Total [# instances]	Limit the total number of times a rule can be invoked. Also used to create one-time-only rules.
Max Use Concurrent [# sessions]	Limit the number of simultaneous sessions passed by the rule. Can be used to session limit busy servers.
Alarm Code [number]	Generate specified alarm number, every time rule is invoked. Can be used in conjunction with alarm triggers to activate email, syslog, or pager alerts.
Dependency Mask	Enable activation of a rule based on an existing firewall cache entry. Used for protocols such as Real Audio, that use different protocols for the control and data portions of the session.
Virtual Private Network	Associate a VPN tunnel (LAN-LAN or Client), with a particular firewall rule.
Authorize Return Channel	Allow return packets from established sessions. Eliminates need to create a separate rule for session responses.
Allow ICMP Replies	Allow ICMP replies for current passed sessions.
SYN Flood	Manage TCP half-open connections. Send TCP "RST" commands to destination hosts that exceed the "incomplete session threshold" after the "Reset Timeout" interval.

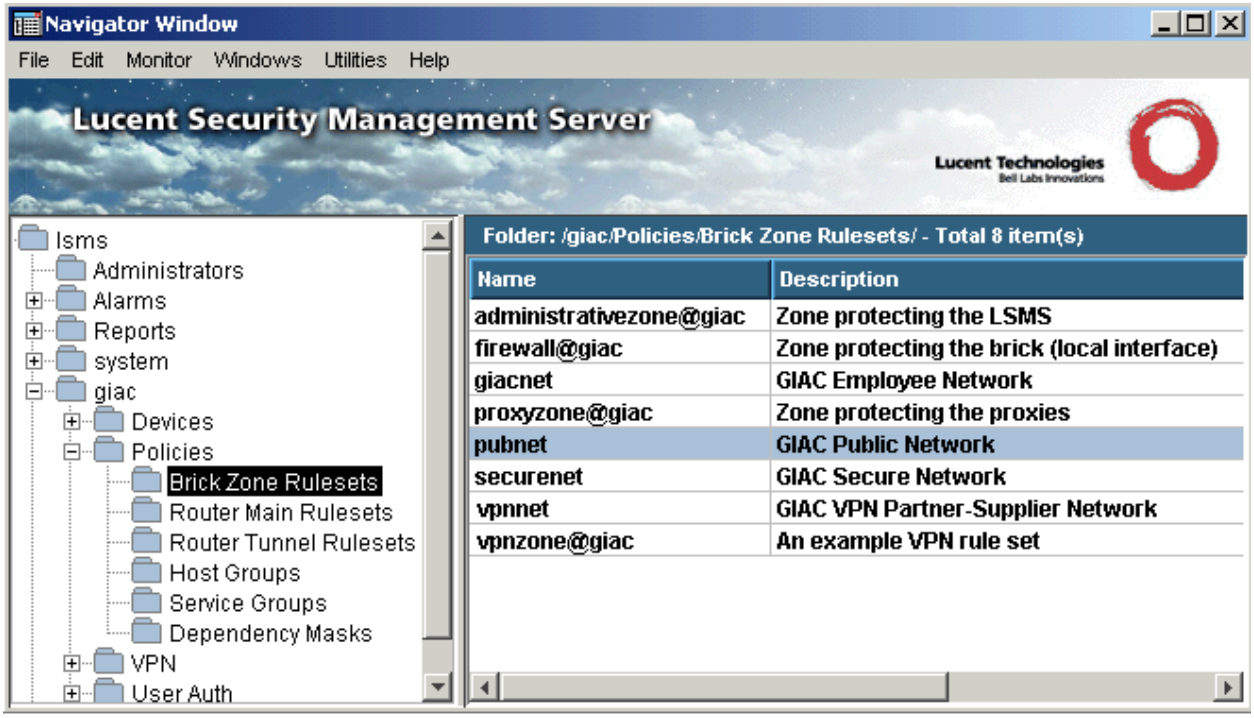
Rule Attributes – Address Translation



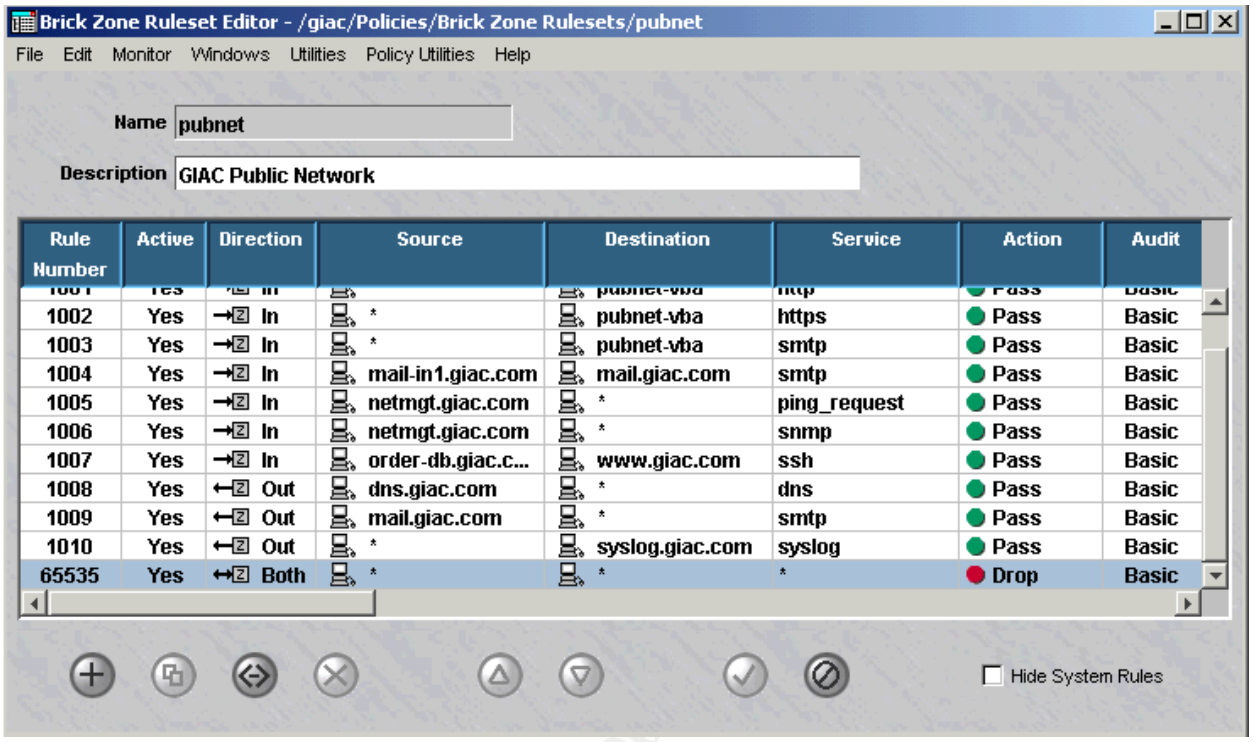
Address Translation Attribute	Description
Source Address Mapping	Mask identity of internal hosts initiating sessions to external networks. Address or host group specifies what servers will handle traffic from external virtual brick address (VBA). Type refers to the ip address assignment. Direct is a one-to-one ip address mapping, that ensures uniqueness for mapped addresses. Pool takes ip addresses as needed, and returns them to the pool when the session is terminated (uniqueness is not guaranteed).
Destination Address Mapping	Mask identity of local servers from external host initiated sessions. Can be used to do server load balancing, and minimize number of registered ip addresses.
Destination Port Mapping	Mask identity of local server ports by binding them to alternate ports.

General Rule Deployment

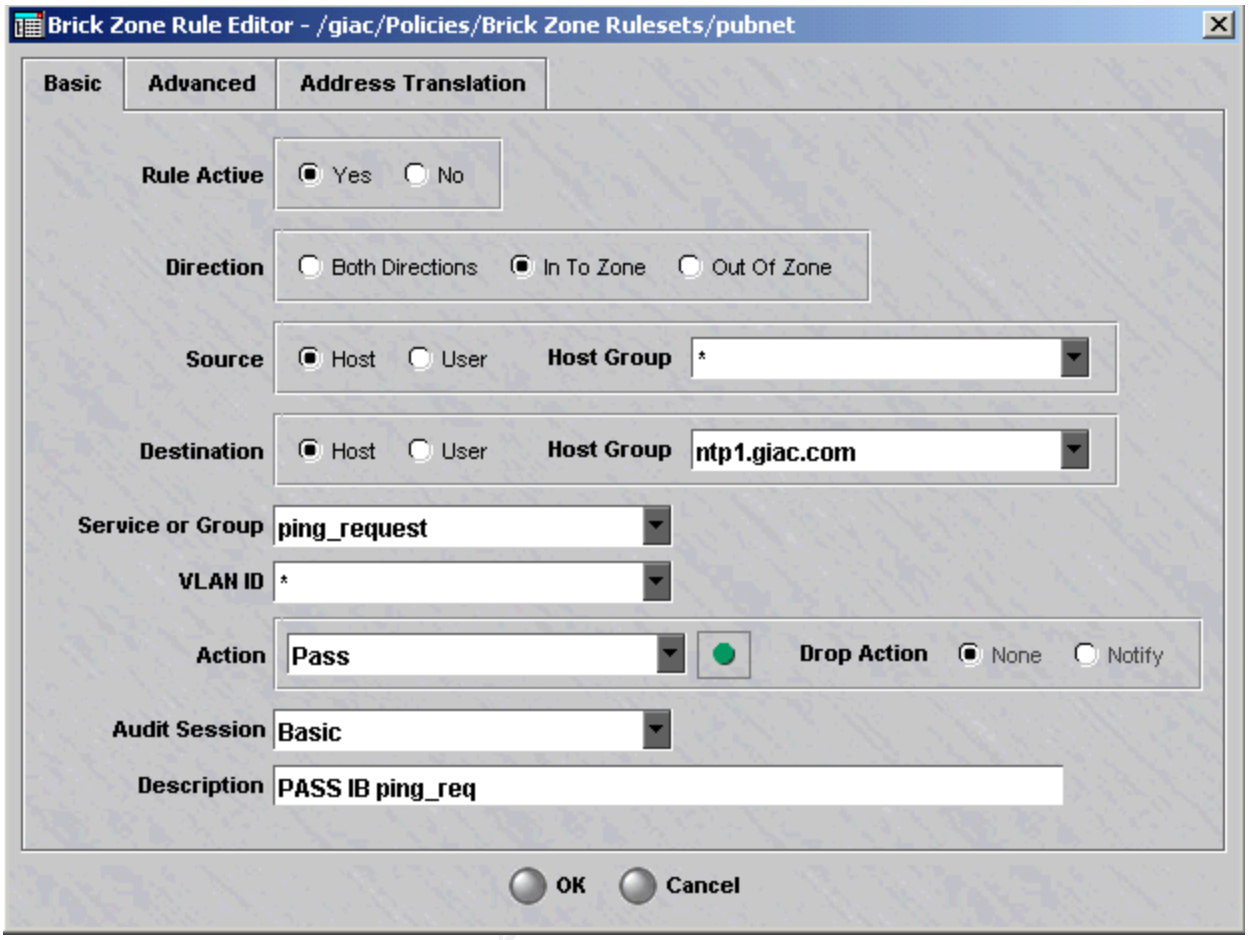
Logon to the LSMS server via the Remote Navigator application and open the GIAC brick zone ruleset folder ("giac/Policies/Brick Zone Rulesets). In the zone window, double-click the appropriate policy (pubnet for this example). This will open the "Brick Zone Ruleset Editor" and display the firewall rules.



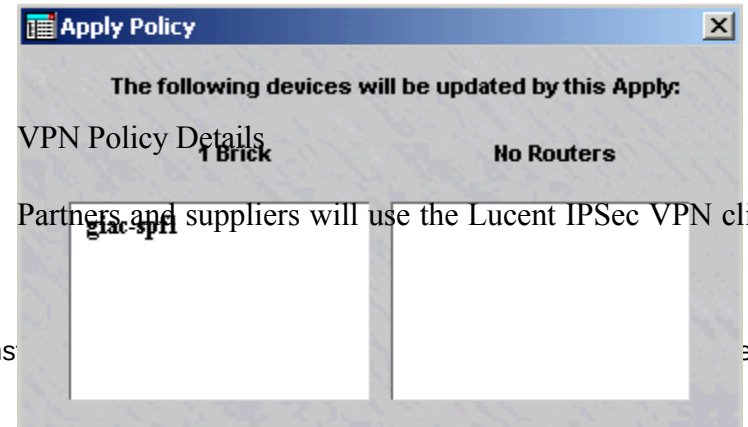
As an example, highlight the last rule in the PubNet policy to insert a new before the last rule. Select the insert icon "+" at the lower left of the Brick Zone Ruleset Editor screen. This will bring up the Brick Zone Rule editor, that will allow the creation of a new rule.



The following screen shows the creation of #1011 that allows inbound ping_requests to go to the GIAC ntp server ntp1.giac.com . The session timeouts for the rule do not need to be manually set, as the LSMS application will default to the longest session timeout of all the protocols specified in the service group. In this case, the session timeout for the rule is set to 10 seconds for the ICMP protocol specified by the ping_request service group.



To add the rule to the PubNet ruleset, click the "OK" button at the bottom of the Brick Zone Rule editor. This will add the rule to the PubNet ruleset. Save and apply the changes by selecting the "File / Save and Apply" menu option from the Brick Zone Ruleset Editor. This will bring up the "Apply Policy" window. The "Keep cache" option is selected by default, and preserves existing sessions. The "Clear cache" option is to ensure the new policy is enforced for all sessions. This may be necessary if the network is currently under attack, and the firewall administrator wants to terminate any existing hacker connections.



VPN Policy Details

Partners and suppliers will use the Lucent IPSec VPN client 4.0.474. Partners and suppliers will

connect to the VpnNet tunnel endpoint via the ether5 VpnNet firewall interface (191.254.15.104). Remote GIAC employees will also use the Lucent IPSec VPJN client 4.0.474 to connect to the GiacNet tunnel endpoint via the ether3 firewall interface (191.254.15.30). The VPN client tunnel will be setup on the GIAC firewall side to use the authentication header (AH-51) protocol. IPSec session integrity will be ensured by AH session header authentication and encryption Data integrity for the application layer will be enforced by 128-bit ssl encryption via https on the GIAC server end. A closed inbound VPN client policy will be enforced by the GIAC firewall on the remote VPN host, to protect the remote VPN host for the duration of the tunnel connection.

ISAKMP Parameters

Attribute	Description
D-H Group	Group 2 : Highest level of authentication. Slower than Group 1 authentication.
Encryption Type	DES CBC : Encryption allowed for international market.
Auth Type	HMAC SHA1 :

IPSec Parameters

Attribute	Description
Protocol	AH-51 : Authentication Header protocol 51.
Auth Type	HMAC SHA1
SA Lifetime (Sec)	14,400 seconds (4 hours). Revoke session after 4 hours. User must re-enable tunnel after this limit is reached.
SA Lifetime (Kbytes)	5,000,000 Kbytes (5 Gbytes). Revoke session after 5 Gbytes transferred. Unser must re-enable after this limit is reached.

VPNnet Rule Hierarchy

Rule #	Description
100-440	System generated rules that enable the VPN and local authentication services.
1000-1006	GIAC custom defined rules.

65535	System generated rule that enforces the allow by exception model. Drops and logs any unmatched (unauthorized connection attempts).

Rule Order

The LSMS system sets the rule order for the system rules. They are automatically inserted before and after the GIAC custom rules to enable the correct VPN operation of the firewall ruleset (the order of these rules cannot be changed by the firewall administrator). GIAC custom rules do not have interdependencies, so they can be arranged in any order. Custom rules have been ordered alphabetically according to protocol (ie https, ping_request, …, syslog).

VPN Ruleset Service Risks

Rule #	Service Protocol (prot/dst/src)	Risk
100	UDP_Encapsulation_Ports udp/501/*	N/A . UDP encapsulation not being used.
101	UDP_Encapsulation_Ports udp/501/*	N/A . UDP encapsulation not being used.
102	UDP_Encapsulation_Ports udp/501/*	N/A . UDP encapsulation not being used.
103	UDP_Encapsulation_Ports udp/501/*	N/A . UDP encapsulation not being used.
305	User authentication. tcp/443/*	External Virtual Brick Address risk via tcp destination port 443.
306	User authentication. tcp/443/*	N/A. Outbound from Virtual Brick Address.
310	tcp/443/*	External Virtual Brick Address risk via tcp port 443.
410	udp/500/*	N/A. Outbound from Virtual Brick Address.
411	udp/500/*	N/A. Virtual Brick Address is the source address.
412	udp/*/500	N/A. Virtual Brick Address is the source address.
420	udp/*/500	External Virtual Brick Address risk via tcp source port 500.
430	IPSec 50/*/*, 51/*/*	External Virtual Brick Address risk via IPSec protocol.
440	IPSec 50/*/*, 51/*/*	N/A. Virtual Brick Address is the source address.
1000	https tcp/443/*	External risk from partner networks via https over authenticated IPSec tunnels.
1001	https tcp/443/*	External risk from partner networks via https over authenticated IPSec tunnels.
1002	ping_request icmp/8/0	Internal risk to VpnNet servers via icmp ping_request from netmgt.giac.com .

1003	snmp udp/161/*	Internal risk to VpnNet servers via snmp from netmgt.giac.com .
1004	ssh tcp/22/*	Iinternal risk to VpnNet servers via ssh from fortune-db.giac.com .
1005	ssh tcp/22/*	Internal risk to VpnNet servers via ssh from fortune-db.giac.com .
1006	Syslog udp/514/*	Internal risk to SecureNet server syslog.giac.com via syslog from VpnNet servers .
65535	*	No risk. Default drop all rule.

Of the risks identified, the most important ones are:

SecureNet Internal

Rule 1006 provides syslog service into the SecureNet service network. This could be used as an entry point from the VpnNet, to access the syslog server to stage broader attacks against SecureNet servers.

VpnNet External

The VpnNet Virtual Brick Address is the tunnel endpoint for the partner and supplier VPN client tunnels. Rules 310, 420, and 430, provide entry points to attack the firewall directly via tcp/443/*, udp/*/500, and IPSec 50/*/*, 51/*/* packets. This could be used to launch DoS type attacks directly against the firewall itself.

VpnNet Rule Testing (Three examples)
General rule testing will involve the following steps:

1. Establish service connection via standard application or nmap;
2. Verify connection via firewall logs.

Rule 1002 Test

Rule Number	Active	Direction	Source	Destination	Service	Action
1002	Yes	In	netmgt.giac.com	*	ping_request	Pass

Ping from netmgt.giac.com to fortune-in.giac.com:

```
netmgt.giac.com$ ping fortune-in.giac.com
fortune-in.giac.com is alive
```

Verify via firewall logs:

0:b:giac-spf1:154256-1:giac:vpnnet:IN:191.254.15.71: 191.254.15.102:0:8:
Pass:e4:e5::1002:1:1::

Rule 1003 Test

Rule Number	Active	Direction	Source	Destination	Service	Action
1003	Yes	In	netmgt.giac.com	*	snmp	Pass

Use nmap to connect to test snmp port:

netmgt.giac.com# nmap -sU -p '161' 191.254.15.103

Starting nmap V. 2.54BETA34 (www.insecure.org/nmap/)
Interesting ports on fortune-out.giac.com (191.254.15.103):

Port	State	Service
161/udp	open	snmp

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

Verify via firewall logs:

0:b:giac-spf1:160552+0:giac:vpnnet:IN: 191.254.15.71:191.254.15.103:57029:
161:Pass:e4:e5::1003:1:1::

Rule 1006 Test

Rule Number	Active	Direction	Source	Destination	Service	Action
1006	Yes	Out	*	syslog.giac.com	syslog	Pass

Use nmap to test syslog port:

fortune-out.giac.com# nmap -sU -p '161' 191.254.15.71

Starting nmap V. 2.54BETA34 (www.insecure.org/nmap/)

```
Interesting ports on netmgt.giac.com (191.254.15.71):
Port            State           Service
514/udp         open             syslog

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

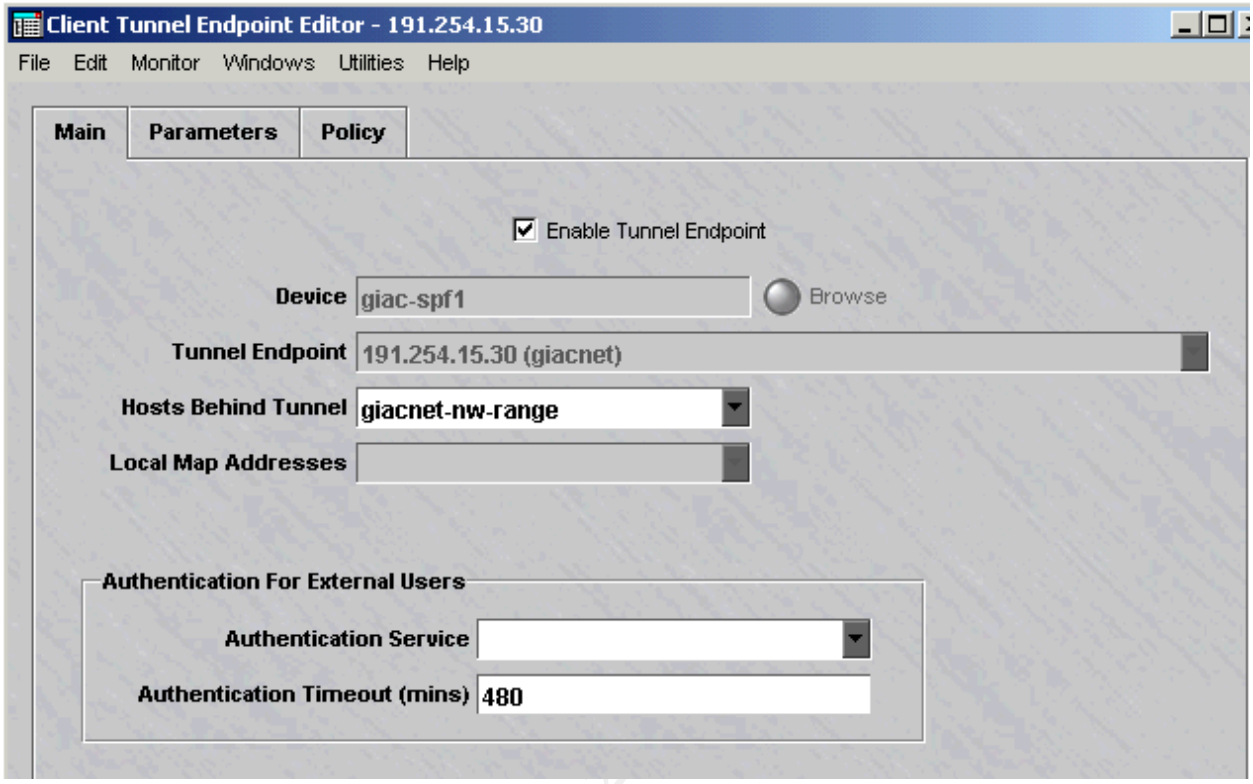
Verify via firewall logs:

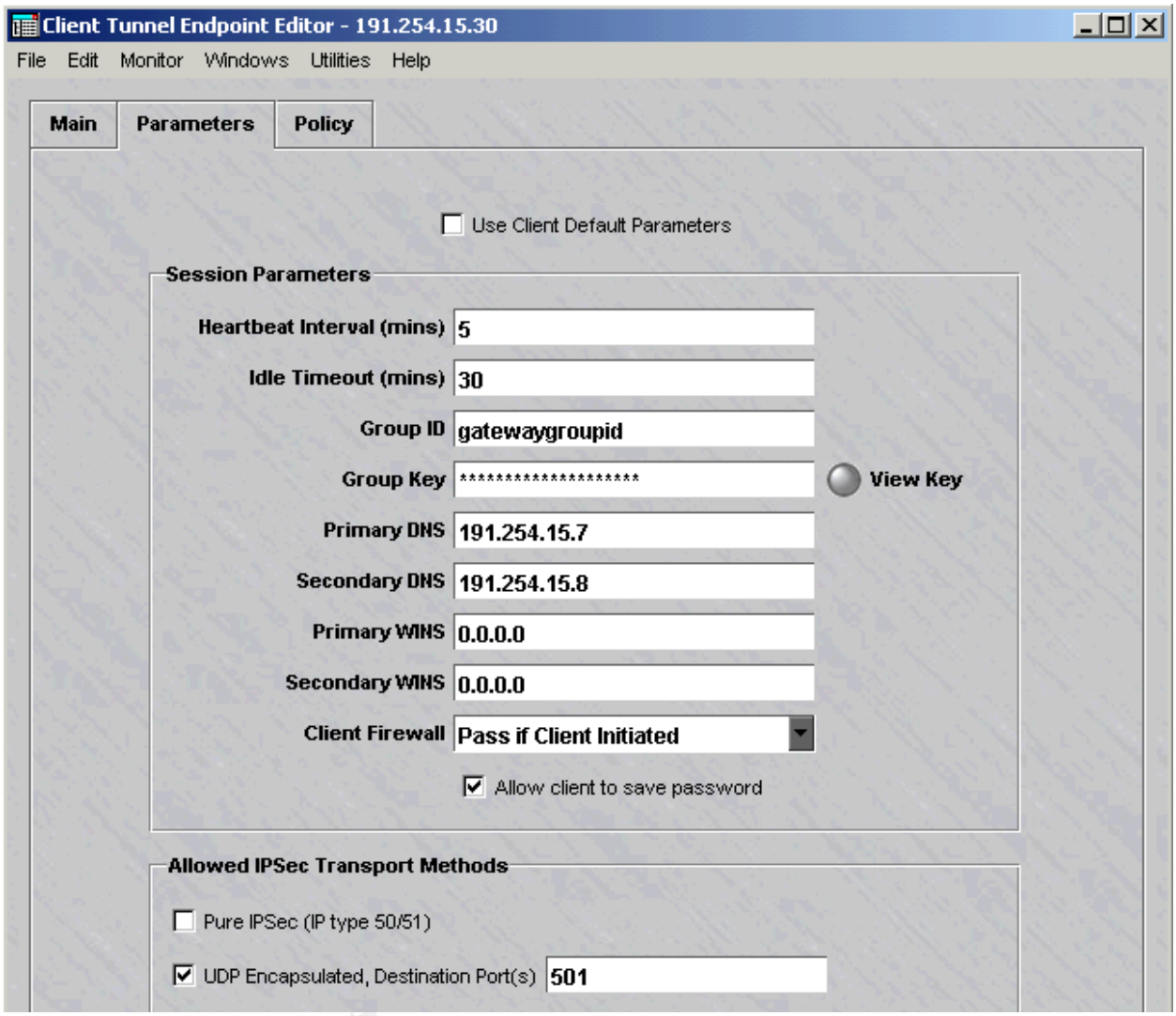
```
0:b:giac-spf1:162501+0:giac:vpnnet:OUT: 191.254.15.103: 191.254.15.71:17:42479:
514:Pass:e5:e4::1006:1:1::
```

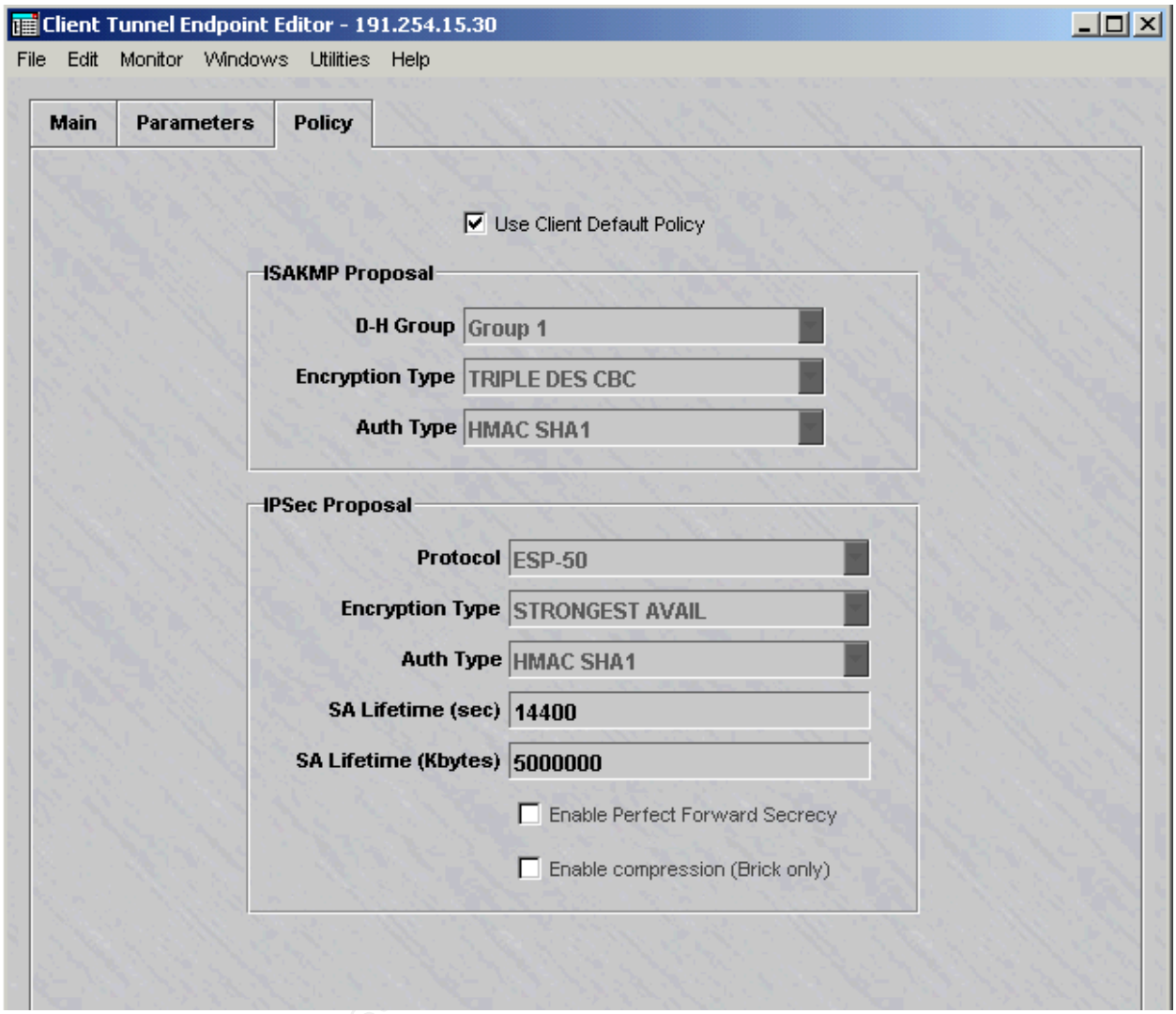
VPN Tunnel Setup

VPN tunnels are configured and setup using the VPN "Client Tunnel Endpoint Editor", from the GIAC / VPN folder. The GiacNet tunnel endpoint is configured as follows:

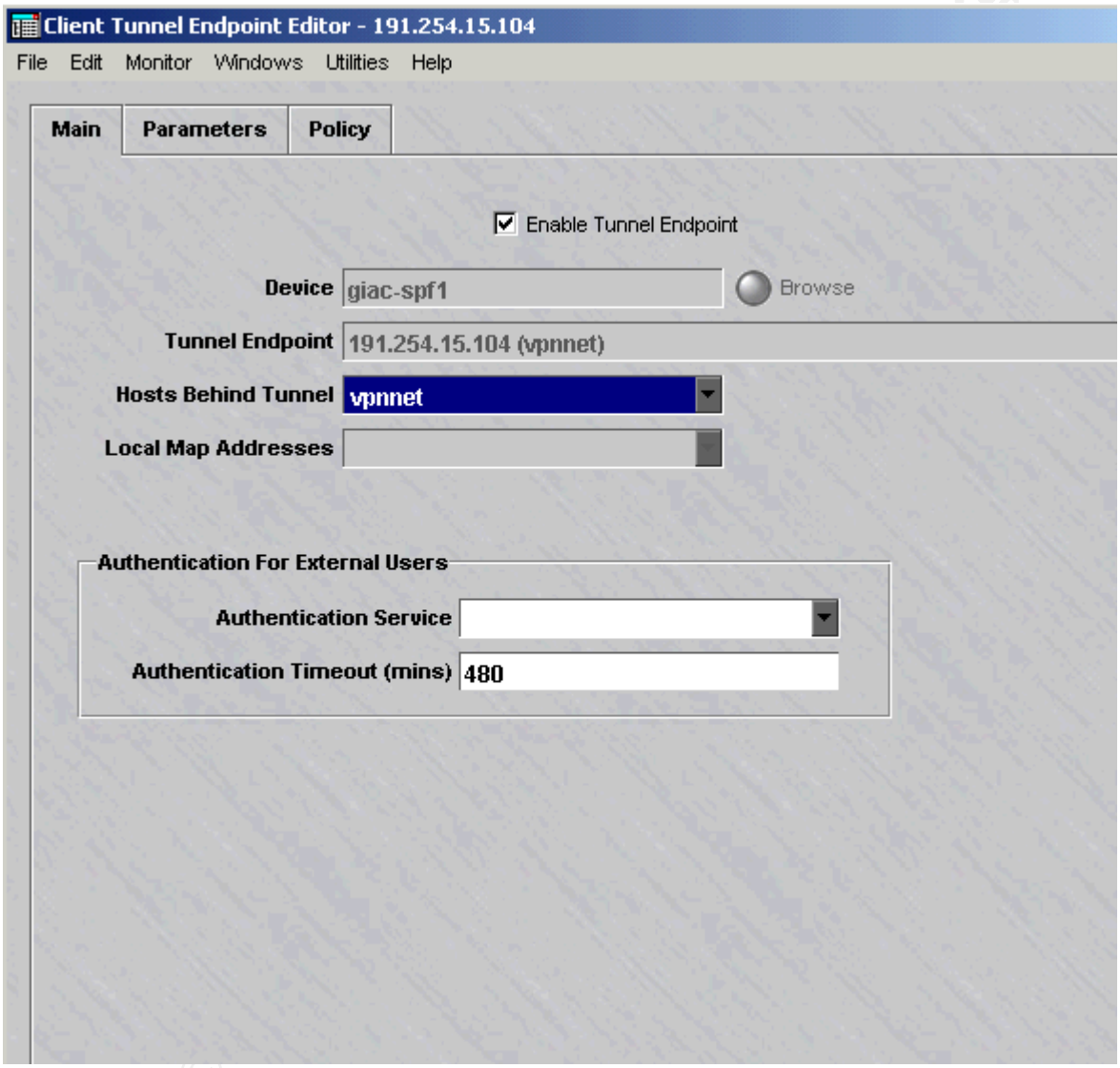
GiacNet Client-LAN VPN Tunnel Endpoint Configuration

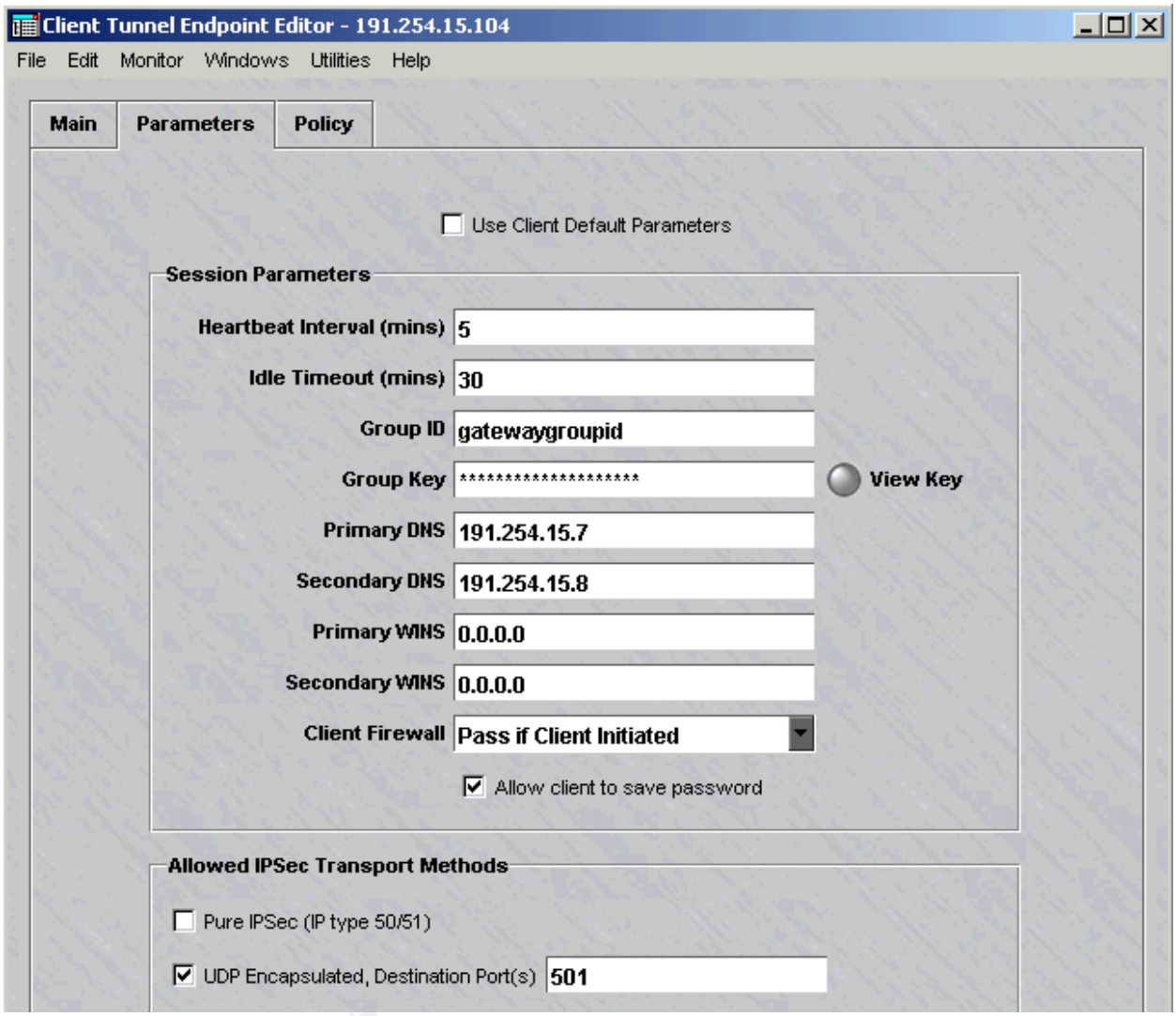


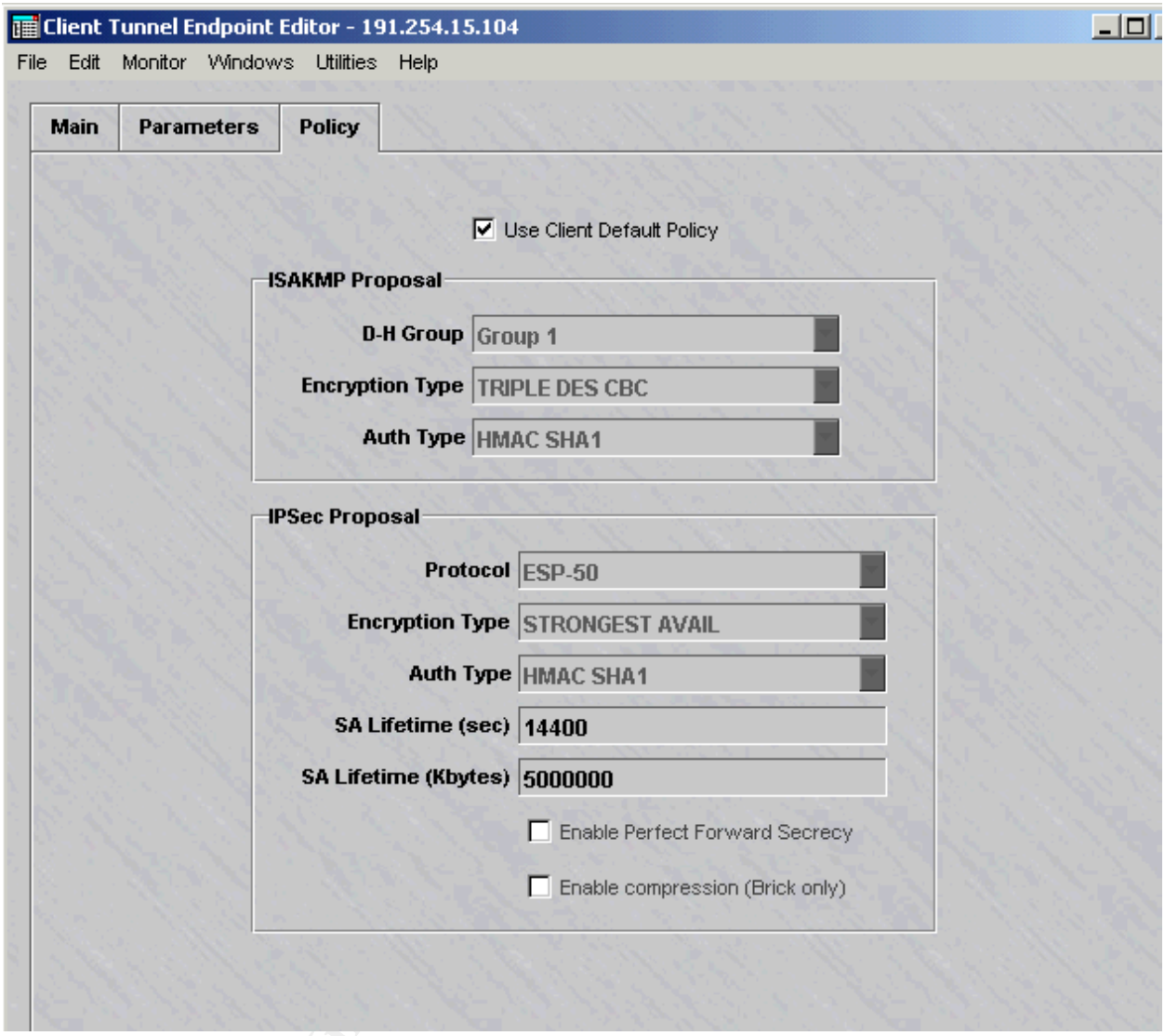




VpnNet Client-LAN Tunnel Endpoint Configuration







GIAC Security Architecture Audit

Audit Plan

The GIAC Enterprise audit will determine the validity of the GIAC firewall ruleset, and the integrity of the Lucent Model 1000 firewall. The audit will be conducted using the "nmap" scanning tool and the firewall logs. Audit activities will be broken up into the following categories:

Firewall Integrity

The GIAC firewall will be tested directly to determine what services are open on the firewall appliance. This will be performed only on the external firewall interface since it is protected only by the "firewall" ruleset. All the other interfaces have the "firewall" and GIAC rulesets applied and will be at least as secure as the "firewall" ruleset alone.

External Ruleset Validation

The GIAC external firewall audit will be conducted from an external ISP (non-partner / non-supplier) network. This will verify the external view of the GIAC network.

Internal Ruleset Validation

The GIAC internal firewall log audit will be conducted to the internet to determine the scope and effectiveness of the internal rulesets.

VPN Ruleset Validation

The GIAC internal firewall log audit will be conducted to the internet to determine the scope and effectiveness of the VPN rulesets.

Time of Day

The GIAC firewall audit will be conducted during normal business hours. This will ensure the appropriate technical staff are on-site to deal with any problems that might arise. Business hour audit will also show the impact of generic scanning activity against the GIAC defense in-depth architecture. This will simulate typical hacker probing activity.

Cost Estimate

Audit

Audit Contractor

80 hours x $200/ hr = $16,000

GIAC Employees Audit Support

160 hours x $50 / hr = $8,000

Disaster Recovery

Per server: $100 / hr for IT support staff

Per GIAC: $1,000 / hr for disaster affecting entire GIAC company

Risks / Considerations

Business Continuity

Business impact will be minimized by ensuring the on-site availability of the IT support staff to ensure service recovery in case the scanning activity brings down the server.

Audit Deployment

The "nmap" scanning tool will be utilized to perform the audit. The following nmap options will be used:

-O Use TCP/IP fingerprinting to guess remote operating system
-P0 Don't ping hosts (needed to scan www.microsoft.com and others)
-sT TCP connect() port scan (default)
-sU UDP port scan
-p <range> ports to scan

Firewall Integrity

External Firewall Integrity (191.254.15.3, 191.254.15.30, 191.254.15.104)

GIAC Firewall Address: 191.254.15.3

Router filter temporarily disabled to allow open access to test firewall IP address.

nmap-2.54b34 -O -P0 -sT –sU -p '1-65535' 191.254.15.3

Nothing returned from scan because "firewall" ruleset applied to all interfaces, prevents packets to the primary firewall device ip address of 191.254.15.3 except for the LSMS server.

GIAC Virtual Brick Address (VPN Tunnel Endpoint):

nmap-2.54b34 -O -P0 -sT –sU -p '1-65535' 191.254.15.104

Operating system could not be determined.

NMAP Results

IP	PORT	SERVICE
191.254.15.104	udp/501	VPN Tunnel UDP_Encapsulation_Ports

GIAC External Ruleset

nmap-2.54b34 -P0 -sT –sU -p '1-65535' 191.254.15.0/24

NMAP Results

DST IP	DST PORT	SERVICE
191.254.15.6	tcp/25	smtp (PubNet)
191.254.15.6	tcp/53	dns (PubNet)
191.254.15.6	udp/53	dns (PubNet)
191.254.15.6	tcp/80	http (PubNet)
191.254.15.6	tcp/443	https (PubNet)
191.254.15.30	udp/501	VPN Tunnel (GIACnet) UDP_Encapsulation_Ports
191.254.15.104	Udp/501	VPN Tunnel (VpnNet) UDP Encapsulation Ports

The nmap results are consistent with the GIAC "PubNet" and "VpnNet" rulesets, and were verified against the firewall logs.

PubNet Verification

Firewall log analysis was used to determine the following outbound services open from PubNet. These results were verified against and are consistent with the closed outbound policy of the PubNet ruleset.

SRC IP	DST PORT	SERVICE
191.254.15.7	tcp/53	dns (GiacNet/external)
191.254.15.7	udp/53	dns (GiacNet/external)
191.254.15.7	udp/514	syslog (GiacNet)
191.254.15.8	tcp/53	dns (GiacNet/external)
191.254.15.8	udp/53	dns (GiacNet/external)
191.254.15.8	udp/514	syslog (SecureNet)
191.254.15.13	tcp/25	smtp (GiacNet/external)

191.254.15.13	udp/514	syslog (GiacNet)
191.254.15.14	tcp/25	smtp (GiacNet/external)
191.254.15.14	udp/514	syslog (GiacNet)

GIACNet Verification

Firewall log analysis was used to determine the following outbound services open from GIACNet. These results were verified against and are consistent with the closed outbound policy of the GIACNet ruleset.

SRC IP	DST PORT	SERVICE
191.254.15.24	tcp/25	smtp (PubNet)
191.254.15.25	tcp/21	dns (External)
191.254.15.25	tcp/80	http (External)
191.254.15.25	tcp/443	https (External)
ALL	udp/514	syslog (SecureNet)

SecureNet Verification

Firewall log analysis was used to determine the following outbound services open from SecureNet. These results were verified against and are consistent with the closed outbound policy of the SecureNet ruleset.

SRC IP	DST PORT	SERVICE
191.254.15.69	tcp/22	ssh (PubNet)
191.254.15.70	tcp/22	ssh (VpnNet)
191.254.15.71	icmp/8	ping_request (ALL Giac NWs)
191.254.15.71	udp/161	Snmp (All Giac NWs
191.254.15.71	tcp/23	telnet (Giac Perimeter Router)

VpnNet Verification

Firewall log analysis was used to determine the following outbound services open from VpnNet. These results were verified against are consistent with the closed outbound policy of the VpnNet

ruleset.

SRC IP	DST PORT	SERVICE
ALL VpnNet	udp/514	syslog (SecureNet)

Audit Evaluation

Perimeter Defense Analysis

The GIAC network is well secured externally via a closed network policy. The nmap scan could not determine any information about the firewall itself (191.254.15.3). The overall GIAC network has a minimal risk exposure from the small number of open services (five: dns, http, https, smtp, VPN), and IP addresses two: all brick virtual addresses).

The internal network is highly segmented and secured. Outbound external access is limited to the PubNet segment (via dns, and smtp) and GiacNet segment via proxy.giac.com.

Primary issue areas include:

GiacNet Proxy

Transfer of corporate information via the proxy.giac.com to internet is possible via web and ftp services.

SecureNet Syslog

GIACnet servers have inbound access via syslog, to the syslog.giac.com server residing on the SecureNet segment. Syslog could be used as an internal attack vector against syslog.giac.com and the SecureNet segment .

VPN Tunnel Endpoints (Virtual Brick Addresses)

GIACnet uses two VPN tunnel endpoints for remote external VPN access. These ip addresses have UDP port 501 VPN services open, and could be a target for external attacks.

Recommendations

Quality of Service

Consider turning on QoS features (at router or firewall), to minimize exposure to distributed denial of service attacks. Packet, bandwidth, and session limiting will greatly enhance ability to withstand denial of service attacks.

Syslog

Consider tightening the syslog rule #1008 from the GiacNet segment to the SecureNet segment to only GiacNet servers. This will reduce the exposure from employee workstations via syslog to the SecureNet segment. Consider running a secure syslog service to increase logging confidentiality.

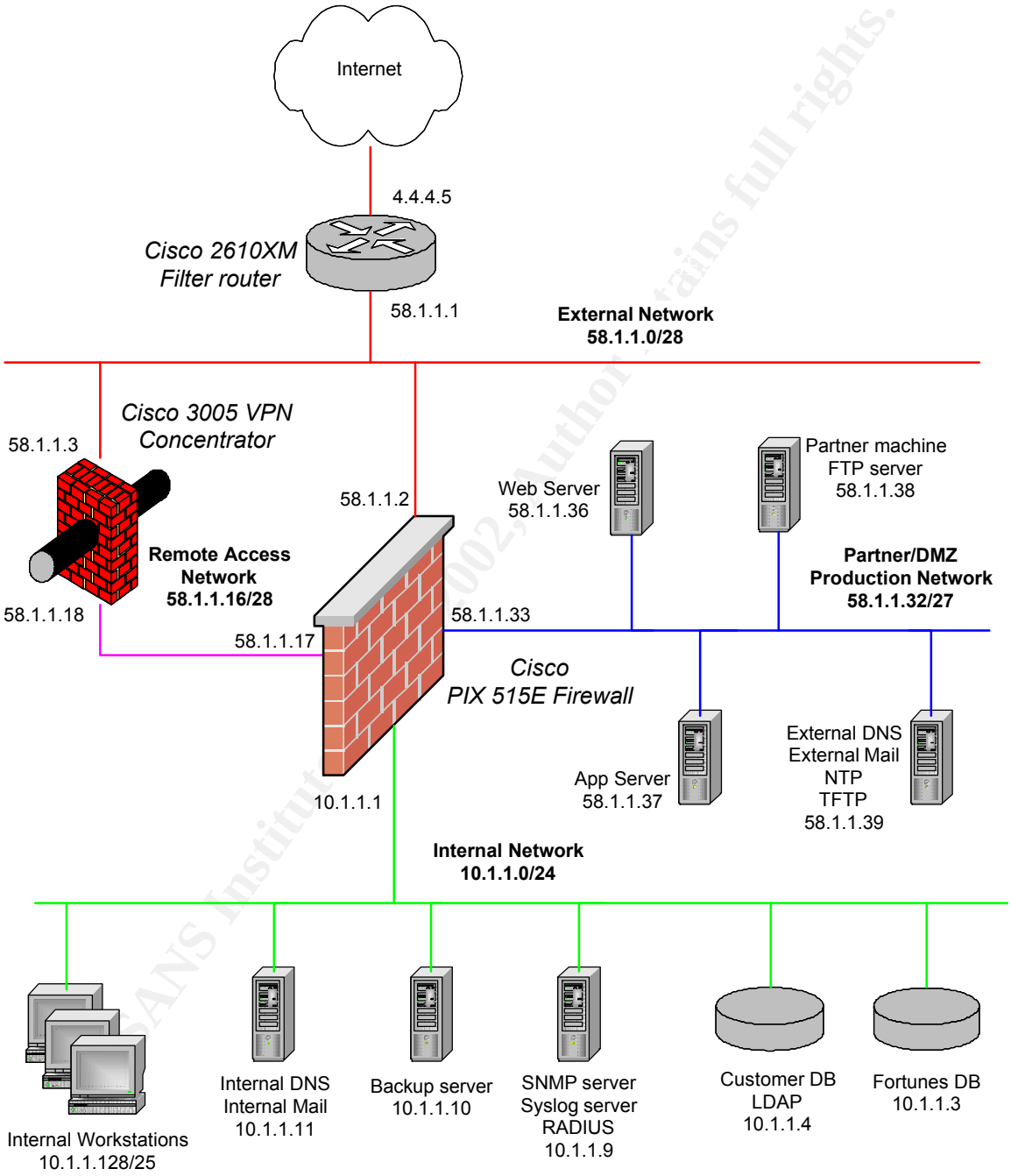
Network Architecture

Significant risk reduction from distributed denial of service attacks can be achieved by upgrading to a higher capacity ISP. Further DDoS risk reductions are possible by moving public web servers to a separate network and ISP connection. Compartmentalizing the public web servers from the GIAC network minimizes the business impact of a DDoS attack on the highest risk external hacker target.

Consider implementing higher authentication levels for VPN and remote access services. Deploying one time password token cards will eliminate the password management problem, and reduce risks associated with password sniffing.

Design Under Fire

The GIAC network design chosen for the design under fire analysis will be based on Steve Keifling's June 5, 2002, GCFW v1.7 design (http://www.giac.org/practical/Steve_Keifling_GCFW.doc) . This network architecture utilizes a Cisco 2610XM border router (IOS 12.1(15), T1 ISP connection), and a Cisco PIX 515E firewall (OS 6.2(1)).



Attack Against Firewall (Cisco PIX 515E)

Research Three Vulnerabilities

Cisco Bug ID CSCdw29965
Security Advisory: Scanning for SSH Can Cause a Crash
http://www.cisco.com/warp/public/707/SSH-scanning.shtml

Vulnerability allows an attacker to send an overly large packet to the SSH daemon, causing the Cisco device to either consume all CPU cycles, or reboot.

Cisco Bug ID CSCdu47003
Cisco Secure PIX Firewall SMTP Filtering Vulnerability
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml

Vulnerability allows an attacker to by-pass PIX "mailguard" feature, allowing attacker to execute blocked SMTP commands.

Cisco Bug ID CSCdt92339
Cisco PIX Firewall Authentication Denial of Service Vulnerability
http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml

Vulnerability allows an attacker to consume all PIX AAA authentication resources, causing a denial of service condition by preventing additional users from authenticating and logging in.

Attack on Firewall

The SSH vulnerability described in Cisco Bug ID CSCdw29965 could be used to launch an attack on the Cisco 515E firewall in Steve Kiefling's network design. It would be a good candidate for attack since a lot of network/system administrators utilize SSH for security and remote access.

The attack could be staged using the CRC32 exploit tool ux2p tool found at the Helsinki University of Technology: http://www.hut.fi/~kalyytik/hacker/uxp2.c

Set the "host" variable to the firewall ip address of "58.1.1.2", and set the "port variable to "22" . Compile program, and then execute via command line using # ./uxp2 . The act of trying to execute the SSH CRC32 exploit against a vulnerable CISCO IOS version, will cause the firewall device to either consume all cpu resources, or reboot causing a DoS condition on the network if it is running a vulnerable IOS version with SSH.

Denial of Service

Given the T1 ISP network connection (1.5 Mbits / sec), an effective denial of service attack will saturate the T1 network link. Our example will utilize 50 compromised cable modem/DSL systems. The DDoS attack can be constructed using the TFN2K DDoS tool , http://packetstorm.decepticons.org/distributed/tfn2k.tgz .

Assuming you have a Linux box, install the tfn2k client on box. Create a file "ownedhosts.txt" that contains the list of IP addresses for the 50 compromised cable modem/DSL hosts.

The following command will launch a flooding attack against the GIAC router ip address 58.1.1.1:

tfn –f ./ownedhosts.txt -c8 –i 58.1.1.1

The above tnf2k client command would tell the (50) tfn2k servers to send a mixed UDP/TCP/ICMP flood attack against the GIAC router IP address 58.1.1.1 (tool claims this type of attack is generally risky for packet forwarding devices such as routers). For complete T1 line saturation, a minimum sustained data rate of 30Kbits/sec for each of the compromised cable modem/DSL hosts would be necessary. Given that the line rates of cable modem/DSL hosts are at least in the hundreds of Kbits/sec throughput range, this rate should be easily achieved by the 50 cable modem/DSL hosts.

Distributed denial of service impact can be lessened (but not eliminated) by using several strategies:

1. Faster ISP connection (DS3, OC-3, …);
2. Higher capacity router (can forward more packets/sec); and
3. QoS (Quality of Service). Implement session/packet/data rate limiting on border router.

The overall affect of these options is to create enough excess network capacity and intelligent packet suppression to weather the DDoS condition, while being able to handle legitimate service requests.

REFERENCES

Baker, Sheridan. The Complete Stylist and Handbook, 2nd Ed. New York: Harper & Row, 1980.

Krutz, Ronald L., and Vines, Russell Dean . The CISSP Prep Guide: Mastering the Ten Domains of Computer Security. New York: John Wiley & Sons, 2001.

Lucent Technologies. Lucent Security Management Server v6.0: Administration Guide, 2001.

Lucent Technologies. Lucent Security Management Server v.6.0: Policy Guide, 2001.

National Security Agency. Router Security Configuration Guide, Report # C4-054R-00, 2001.

Peltier, Thomas R. Information Security Risk Analysis. Boca Raton: Auerbach, 2001.

URL's

DDoS Tools (TFN2K)

http://packetstorm.decepticons.org/distributed/tfn2k.tgz

DDoS Tools: SSH CRC32 (uxp2)

http://www.hut.fi/~kalyytik/hacker/uxp2.c

Cisco

http://www.cisco.com

Lucent

http://www.lucent.com/security