Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 3.0 (January 28, 2004)

David Levant

August 17, 2004

Table of Contents

Abstract

The below assignment is composed of four parts

1. **Security Architecture**
   The purpose of this part is to design security infrastructure for "Giac Enterprise".
   Giac Enterprise is not large company located in one geographical location that has e-biz for selling sayings for fortune cookies. It has business partners, travel sales persons, telecommuters and regular requirements to fulfill employee's needs for e-connectivity like e-mail, web surfing, etc…
   My design should allow convenient network work environment for employees and partners, easy access for customers willing to purchase through company web site and in parallel to minimize to minimum the chance for malicious attacker make damage to the company. The damage can be done by stealing companies intellectual property or distracting e-biz (e.g. by DoS attacks)
2. **Security Policy applied on the main building blocks**
   The purpose of this part is to provide information on how the Routers and Firewalls should be configured from Security point of view to compliment the design made in part 1.
3. **Design under Fire**
   The purpose of this part is to suggest a way to perform attack against design proposed in one of the previous works. I chose to perform attack against design by Marc Panet:
   http://www.giac.org/practical/GCFW/Marc_Panet_GCFW.pdf
   The attack should be realistic and I will use existing tools and already published vulnerabilities.

4. **Future state of security technology**
   In this part, I will suggest framework for Security Management. The Framework is needed mainly for large corporate with segmented network and large number of security device like Firewalls, IDS, Routers with ACLs, IPS …

Assignment 1 – Security Architecture

Company Overview

GIAC Enterprises is an e-business which sales online fortune cookies sayings. The company have ~50 employees located in headquarter and about 20 sales people. The e-Biz done through web home page that allows customer to purchase cookie sayings with on-line transactions. Cookie sayings are developed

by two business partners that are supplying the sayings with on-line transaction from their enterprise network.
Most valuable asset of the company is customers data (personal information as well as credit cards numbers and special prices) that many competitors would like to get.
Maximal traffic to/from Internet (on the link to ISP) - 8Mbps, as measured for spikes during prime time.
Company management decided to spent decent amount of $$$ to ensure “non stop” e-commerce and no leakage of customers credit cards and personal information.

Company Requirements

1. Provide non stop access for customers to the company web server for e-Biz. Required up-time: 99.99% (at most 60 minutes downtime/year)
2. Ensure customers transaction security & privacy
3. Protect customers/transactions database from unauthorized access
4. Allow sales persons and teleworkers to access company internal network
5. Allow partners to supply sayings in secure way “over the wire”
6. Allow inter-company e-mail exchange
7. Allow company employees to access business related web sites (~100) on the Internet from company network. FTP downloads from Internet should be allowed as well.
8. Provide basic protection from viruses, worms and e-mail spam

Conceptual Design Guidelines

Overall guidelines: Stateful Inspection Firewall (FW) will be used. NAT will be used for DMZ servers. No direct connectivity from LAN to Internet will be allowed – only through DMZ servers.

Firewall

First decision is if to use commercial FW Vs. freeware FW

Option	Advantages	Disadvantages
Commercial Firewall	Ease of management, better support, training materials	Cost – initial and ongoing (support, patches, new versions)
Freeware Firewall	Cheapest solution	Complicated management, No vendor support, need to follow up on related vulnerabilities, patches, etc…

Because company IT have only one Network engineer that in charge of all the Network security as well, decision to choose the easiest managed (GUI) and best supported FW.

Recommendation: to use Checkpoint Firewall-1 on general build server running Checkpoint OS – SecurePlatform (hardened Linux, supported and maintained by Checkpoint)

Two option for Firewall design:
1. One Firewall : Inbound and Outbound DMZ traffic going through same physical Firewall
2. Two Firewalls - internal and external, DMZ subnets between the two:
Company LAN ----- Internal FW ----- DMZ ----- External FW ------ Internet

Option	Advantages	Disadvantages
One Firewall	Cost	Less secure solution. Vulnerability in Firewall software will expose the internal network as well
Two Firewalls	More secure solution. Allows implement security in depth by implementing Firewalls from two different vendors – vulnerability in one will not open the door through the second	Support two different products, more complicated troubleshooting. Additional cost

In my opinion the extra security in additional Firewall layer is not significant. The most important data on internal network is saved on one SQL server and for security in depth approach we can improve the security of this server instead of installing additional FW.
Recommendation: to use one Firewall

Robustness and Durability

To fulfill 99.999% uptime request we need to give answer to systems reliability (e.g. H/W failures or ISP failures) and DoS attacks durability.
Network reliability: For such uptime the only option is to use redundant network equipment – Routers, Switches and Firewalls -connected to two different power circuits. Because ISP's uptime is usually less then our requirement, we will use two circuits to two different ISPs. ISP redundancy can be implemented in two main ways:

Option	Advantages	Disadvantages
Router to get all BGP routes from ISP router	Best routing decisions (which ISP link to use) for outgoing traffic	Need quite strong routers with enough RAM, to get all routes from ISP – extra $$$
Router to get default route from ISP router (and advertise it to our	Simple routing tables on the router. No need for strong router	Outgoing traffic will go through one ISP only

second router to cover the case of ISP failure)		

Recommendation: Use full BGP routing tables for better customer response times and probably better load balancing between two ISPs.

Web Server reliability: Two redundant servers will be used. To perform load balancing between the servers three main options can be used:

Option	Advantages	Disadvantages
Checkpoint FW to perform the load balancing	Ease of configuration. All configurations (security and redundancy) in the same policy	Extra load on the FW. Capability that will not be available in case of FW brand change
Dedicated load balancing appliance (e.g. BigIP or RAD)	Product independent – will work for any choice of OS and web server software	Additional cost and maintenance
Microsoft NLB software	No performance impact on the FW	Extra load on the server, complicates configuration and troubleshooting. Will work only on Windows

Recommendation: configure load balancing on Checkpoint FW. Because of the concern regarding load on the FW, MRTG to measure FW CPU should be created and HTTP response time should be measured (open source tools like openNMS can be used for this purpose as well). Cisco RTR HTTP can be configured on the router to perform response time measurements. In case of trend in CPU increase and/or response time increase over time, other option might be considered. In any case use strong dual CPU server with Checkpoint SecureXL feature to increase performance and allow more efficient usage of both CPUs.

DoS durability: For 99.99% web site uptime requirement we need to ensure durability for DoS attacks against bandwidth of ISP link, Routers facing ISP, Firewall and Web servers. There is no perfect way to completely prevent damage, but we can do couple of steps to reduce risk:

- QoS that ensure bandwidth for port 80 traffic to web servers should be configured on ISP routers (if they agree… If not at least on our routers)
- Detection of DoS attacks (especially on port 80) and **automatic** appropriate ACL implementation on the routers to block attacking IPs
- QoS on the Firewall that will not allow too much traffic on port 80 to web servers (according the server specifications)
- Have agreement with ISP that will allow us to request ACL implementation on ISP routers to protect our link

- To use stronger Routers to allow effective filtering during DoS attack

Remote Access for Teleworkers and Sales People

Main two options is to use dial-up line to RAS server or VPN. VPN will give much better performance and probably will be more secure solution.
Recommendation: use remote VPN

Three main options for VPN gateway

Option	Advantages	Disadvantages
VPN gateway runs on the Routers connected to ISP	Traffic through the Firewall will be already decrypted – filtering can be done, better logging, … No additional $$$ needed	Extra load on the Router. Less secure – no filtering device in front, more vulnerable to DoS attacks
VPN gateway runs on the Firewall	No additional $$$ needed. All configurations – security and VPN in one place – easier maintenance, auditing log analyzes	Extra load on the Firewall. No flexibility in VPN brand choice – tight to Firewall vendor
VPN gateway runs on dedicated appliance	VPN gateway product decision not tight to Firewall product. No extra load on Firewall. Additional filtering device before the VPN gateway – better filtering options	Additional $$$ and support of additional box. VPN access policies configured in different place than security policies

Recommendation: Run VPN gateway on the Firewall. It will save $$$, reduce management overhead and will allow defining all security policies in one place. Monitor Firewall performance to ensure that no performance degradation trend is observed

Main choices for client authentication

Option	Advantages	Disadvantages
Local authentication on VPN server	Easiest way	Need to maintain passwords on the VPN gateway and all the password renewal process. Remote clients should remember additional password
Authentication on LDAP	Can be used by other	Less secure –

server	applications (e.g. Microsoft authentication). Least maintenance needed (in assumption that LDAP server exists anyway for LAN purposes)	obtaining/breaking MS password will allow attacker to VPN to local network.
Authentication on ACE server (+ secure ID)	Very secure	Need to bring up ACE infrastructure. Very expensive
Usage of Certificates	Probably most secured way. Users does not need to remember passwords	More complicated configurations and sustaining of additional features. Troubleshooting more complicated as well.

Recommendation: To reduce overhead from Network engineer use existing LDAP server. The little bit reduced security seems as less important in this case, if we will ensure good protection of the SQL server holding the confidential data and make good IDS and logging systems.

Partners Access

The standard way to provide partner access is to use site to site VPN and allowing the partners connect to specific servers on dedicated VLAN. However in our case the partners need to post sayings only, so site to site VPN seems as overhead.
Recommendation: Build SSH server in DMZ and allow partners to upload sayings with FTP over SSH to dedicated directory. SSH should listen not on standard 22 port, but arbitrary (e.g. 9013). The server should be on dedicated VLAN to reduce the risk of attacking from the server if it going to be compromised.

SQL Server

The server holds most confidential data.
Recommendation: Physical access to the server should be restricted. Backups should be done on directly connected tape and not through the network. The server should be located on dedicated VLAN with Access Lists on the tcp1433 and udp 1434 from required hosts only (1433 is default port. If applications will support can be configured to listen on different port). All non SQL services on the server should be shut. Updated anti-virus should be installed. Personal Firewall/host intrusion detection on the server is an option. Constant follow-up on the latest patches should be done on daily basis (utility like Shavlik HFNetChk.exe can be used. Scheduling to run this utility will reduce drastically the management overhead)

DNS Services

From security point of view no other reasonable option than two DNS servers – internal and in DMZ – can be proposed…
Recommendation: Install additional DNS server in DMZ that will hold information about external (NATed) addresses of DMZ servers only and will act as "proxy" for internal DNS server. Internal DNS will be configured with "forwarders" option. Use dedicated server and not one server for multiple purposes (e.g. mail, proxy, http, …)

Mail Services

Recommendation: Install SMTP server in DMZ. Consider to use Postfix or smap instead of full featured (and thus more vulnerable) Sendmail for incoming SMTP connections. Both mentioned programs can then relay the messages to internal Exchange server.

Internet Access from GIAC Enterprise Network

The requirement for "business related web sites (~100) on the Internet from company network" enforces us to make URL content filtering.

Option	Advantages	Disadvantages
Use 'security server' capability of Checkpoint Firewall-1	All security policy configurations in one place – ease of management	Extra load on the Firewall. HTTP performance might degrade. Change of Firewall brand (from Checkpoint) will enforce change in Proxy design
Use dedicated HTTP proxy server (e.g. Squid or NetCache)	Reduce load from Firewall. Server can be used as FTP, Telnet or SOCKS proxy as well.	Additional server to manage and carry for security. Additional $$$, especially if commercial product like NetCache is used

Recommendation: Install dedicated server, mainly because we already added VPN and load balancing features on the Firewall. Use freeware Squid application to reduce cost. Install on the same server ftp-gw, telnet-gw, general plug gateway application and SOCKS proxy. This will allow flexibility in the future to fulfill special requirements. Ensure "one way" configuration – so only request from internal network addresses to Internet will be served. Nice features like virus and malicious code scanning coming with commercial proxies are less important in our case, because of very limited URL list that can be accessed. Because proxy application is not running on the Firewall, in the future it will be easy to replace our freeware proxy with commercial one, if the need will come

Protection from viruses, worms and e-mail spam

The requirement is for basic protection, so main effort should be done on anti virus updates and patches. Teleworkers notebooks should be protected by personal firewall as well. Worms are in general using very aggressive IP scans and usually to IP address ranges that are not part of company LAN. Such pattern can be easily identified by IDS. Script that map source IP address of the attacker to Switch port[1] and disables it with appropriate alert should be written.
SmartDefense capability of Checkpoint Firewall-1 should be activated. Updates according Checkpoint advisories should be performed on regular basis.
For defense in depth, recommended to use two different antivirus products – for servers and for clients.
Patch/service pack/dat files revision versions of the clients should be monitored. The simplest is to write VB script that will read from registry the relevant version numbers and send the data to central repository. The script should be scheduled to run every X hours.
Develop emergency response process that can mitigate the risk of worm infection as soon as appropriate alerts received from IDS. One of the options is to prepare ACL on the LAN router that will block all the traffic except to the servers, and attach it to the interface as soon attack identified.
Regarding e-mail spam, no magic tool exists. Manage self created "spam" subject lists on SMTP server is extremely human intensive task. Commercial products for mail scan are in general very expensive. Usage of public databases like orbz.org for real time "black lists" is risky, because your Sendmail can block outgoing/coming mails to partners that entered to black list because of spammers spoofing activity. Recommendation is to do nothing in phase 1. If spam mail will become real disturbance, consider to purchase commercial product for stop spam and virus e-mail scanning like eSafe from Aladdin or freeware like SpamAssassin (www.spamassassin.org) .

IDS

Recommendation: Install two IDS systems connected to "SPAN" port on DMZ switch and LAN switch (all Cisco Catalyst switches supports span port that "see" all the traffic passing on the switch bus). As well use SmartDefense IPS capability of Checkpoint Firewall-1 including update subscription.
Two options for IDS product:

Option	Advantages	Disadvantages
Use commercial product (e.g. Cisco IDS)	Automatic updates are sent for every new signature. Vendor support	Cost: initial and on-going for support. Less features supported and less flexible in configuration.
Use open source	Highly flexible in	More specific

[1] "show ip arp" on the Cisco router will map IP addresses to MAC address and "show cam dynamic" on the Cisco switch will create mapping of MAC to switch port. From those two, mapping of IP to switch port can be obtained.

application - SNORT	configuration. Supports many features including network traffic anomalies	knowledge\training needed. No automatic updates, need to be “on top” of the new vulnerabilities and SNORT updates. More difficult management\sustaining

Recommendation: use SNORT as the IDS system. The added complexity in management is less important than the ability to make exact configuration suited for the environment and reduce drastically false positives alerts. (Saving $$$ as well ☺)

Logging/Alerting

Highly recommend to have one system for all alerts. Commercial systems like HP OpenView or NetView can be used. Open source OpenNMS (http://www.opennms.org) available as well. Log aggregation is complicated task, but if alerting system will be properly configured, then each log examination can be done on dedicated system (syslog for routers, smartview tracker for firewall, IDS, etc…) . Syslog can run on OpenNMS system as well it will be the target for snmp traps sent by Firewalls.

NAT policy

Because access to/from Internet allowed to/from servers in DMZ only, we can use static (1:1) NAT on the Firewall for each DMZ server. DMZ servers should be configured with addresses from private IP scope and Checkpoint Firewall will perform NAT.

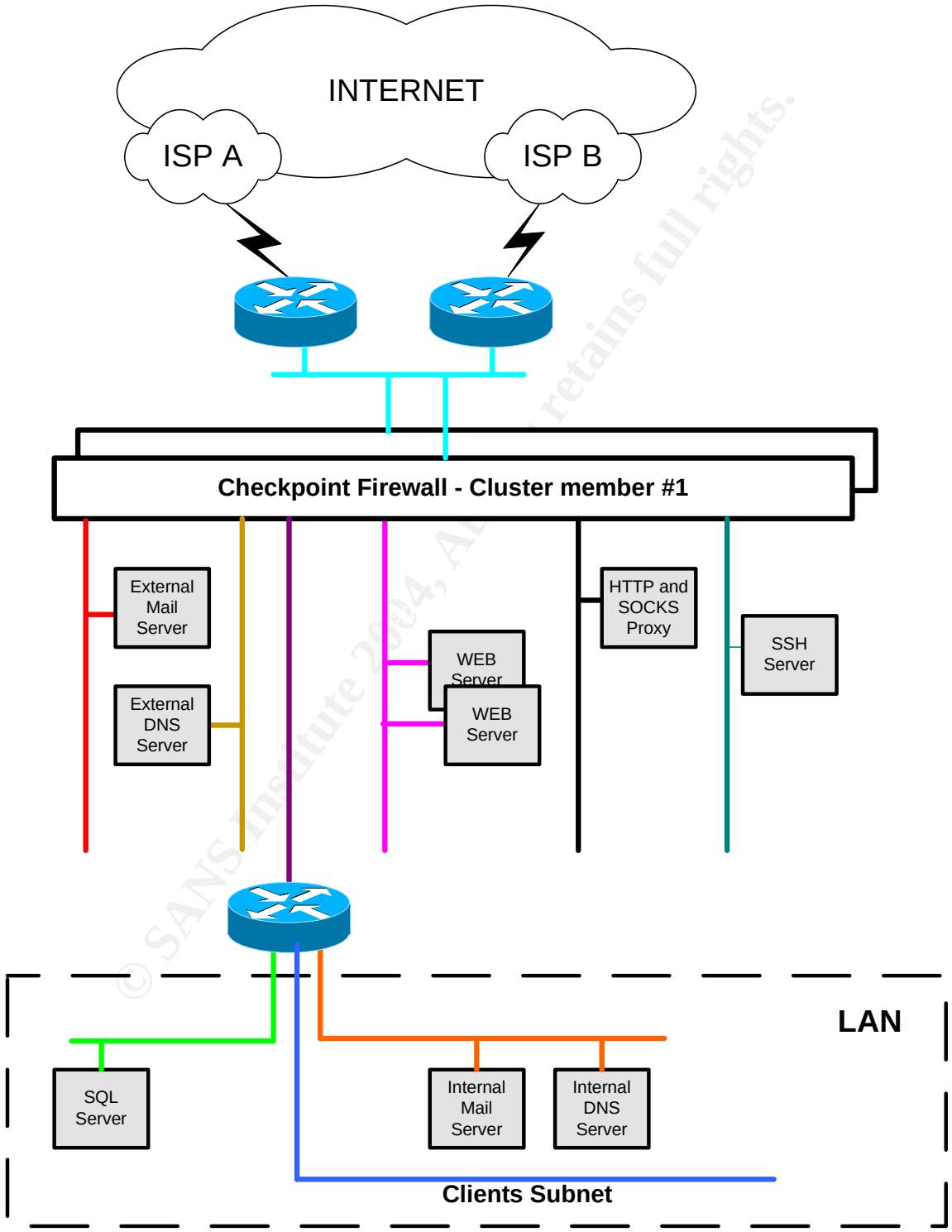
Summary of the recommendations according to the requirements

1. *“Provide non stop access for customers to the company web server for e-Biz. Required up-time: 99.99%”*
    a. Use redundant Network equipment for DMZ
    b. Use connection to two different ISPs
    c. Use two (or more) web servers with load balancing
    d. Prepare detection systems and emergency response process for DoS attacks. ISP should partnership with you in the process (mainly implementation of ACLs on ISP routers)
2. *“Ensure customers transactions security & privacy”*
    a. Use https
    b. Register your company in Public Certificate Authority (e.g. VeriSign), so customers will be able to verify connection to GIAC site
3. *“Protect customers/transactions database from unauthorized access”*
    a. Harden SQL server
    b. Keep it on separate subnet with appropriate ACLs

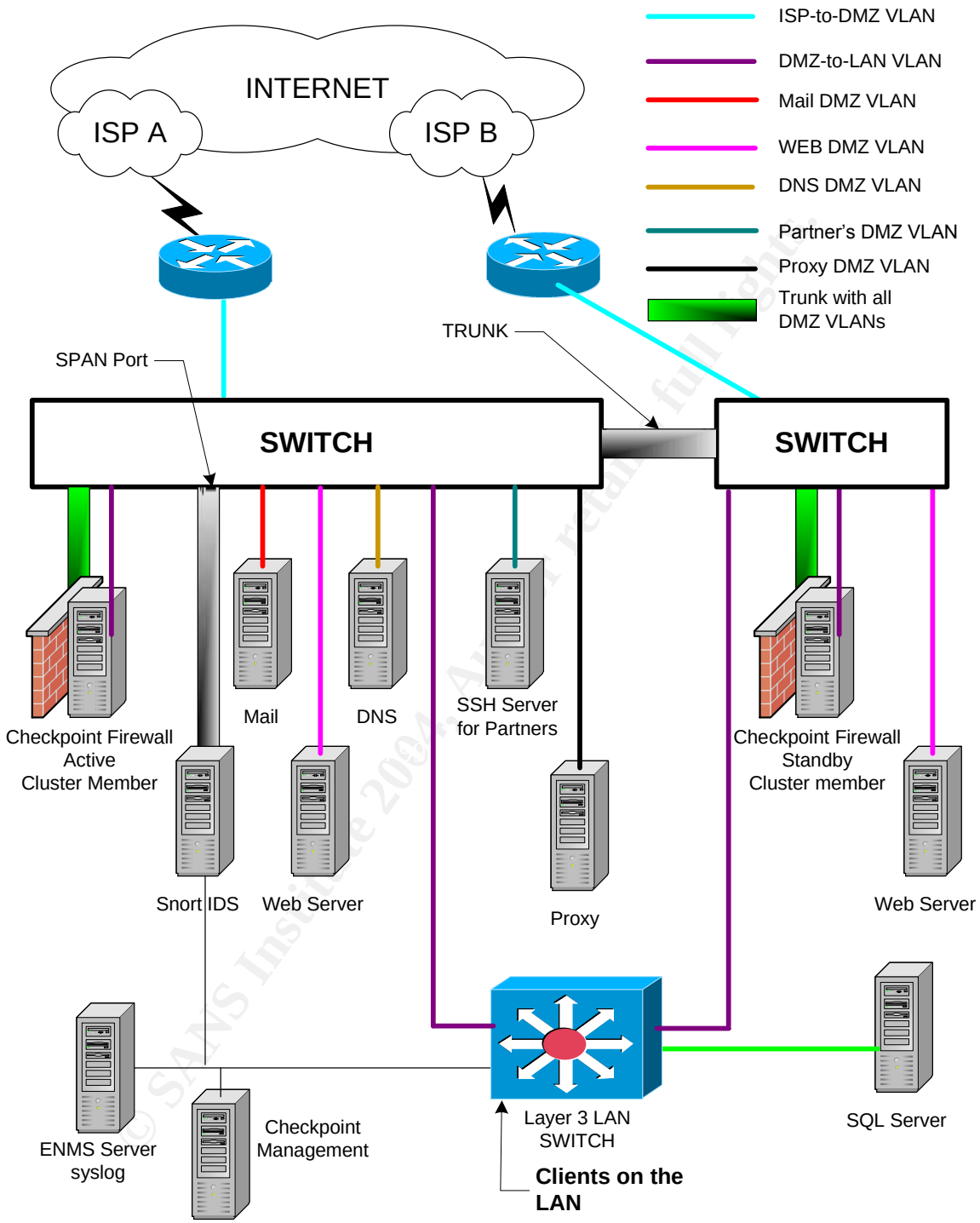
    c. Physically locate in confined space
4. *"Allow sales persons and teleworkers to access company internal network"*
    a. Use remote access VPN
    b. Use existing LDAP server for authentication
5. *Allow partners to supply sayings in secure way "over the wire"*
    a. Install hardened SSH server in DMZ and let the partners 'ftp put' sayings over the SSH to the server
    b. Configure SSH to listen on some high port and not 22
6. *"Allow inter-company e-mail exchange"*
    a. Install Mail server in DMZ
    b. Use simple application like Postfix on DMZ server
7. *"Allow company employees to access business related web sites (~100) on the Internet from company network. FTP downloads from Internet should be allowed as well*".
    a. Install Proxy server in DMZ and allow Internet access only through Proxy
    b. Configure URL access lists on the Proxy server
    c. On the same server install ftp-gw for FTP Internet access
8. *"Provide basic protection from viruses, worms and e-mail spam"*
    a. Define on going patching process and execute it (for OS/application patches and antivirus dat files)
    b. Install personal firewall on the laptops of remote users
    c. Use IDS to identify attacks and disable switch port of attacking host
    d. Define emergency response process that will mitigate the risk of infection as soon worm pattern identified by IDS.

Network Design

Network Drawing – Layer 3



Network Drawing – Layer 2



Few clarifications:

- Each DMZ subnet defined on different VLAN for security purposes. The Default Gateway for DMZ servers is Firewall.

- Firewall have 3 physical NICS:
  - DMZ-to-LAN NIC. Traffic which destination is LAN will go through this one (accomplished with static routes on the Firewall for all LAN subnets)
  - Sync NIC. Cross cable connected to this NIC and connecting both Firewalls. This sync network is used for connection tables exchange between primary and secondary routers for transparent failover
  - DMZ NIC. One physical interface, but all the VLANS including ISP-to-DMZ defined on it. So on the firewall we will see 6 virtual NICs

    ifconfig command on the Firewall (I am showing only first two Vlans ISP-to-DMZ (vlan 43) and WEB-DMZ (vlan 44))

```
eth1      Link encap:Ethernet  HWaddr 00:0B:CD:4A:C2:28
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:530340116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:516956273 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2138883573 (2039.7 Mb)  TX bytes:902486834 (860.6 Mb)
          Interrupt:5

eth1.43   Link encap:Ethernet  HWaddr 00:0B:CD:4A:C2:28
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:96675527 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62438183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:528839331 (504.3 Mb)  TX bytes:3042711634 (2901.7 Mb)

eth1.44   Link encap:Ethernet  HWaddr 00:0B:CD:4A:C2:28
          inet addr:192.168.2.33  Bcast:192.168.2.255  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4332003 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:828039160 (789.6 Mb)  TX bytes:104430 (101.9 Kb)
```

- Port on the Switch that the Firewall trunk connects to defined as dot1q trunk with all 6 DMZ Vlans (except DMZ-to-LAN) allowed
- Security management network defined on LAN Layer3 switch. Checkpoint management server and ENMS server that is running syslog as well connected to this network. ACL to restrict access to this subnet defined.
- Internal Mail server and Internal DMZ servers are not shown. They are connected to dedicated LAN VLAN. Domain Controller located on the same VLAN as well. Basic ACL protects the Vlan and internal IDS system monitors it.

IP Scheme

Internal Addresses

Hostname	IP Address	Subnet Mask	Default Gateway	Interface	VLAN	Switch
ISP to DMZ	192.168.2.0/28	255.255.255.240			700	

Router1	192.168.2.1	255.255.255.240	ISP Router	FastEthernet 0/1	700	DMZ Switch Primary
Router2	192.168.2.2	255.255.255.240	ISP Router	FastEthernet 0/1	700	DMZ Switch Secondary
Routers HSRP address	192.168.2.3	255.255.255.240				
Primary Firewall	192.168.2.4	255.255.255.240	192.168.2.3	eth0.700	700	DMZ Switch Primary
Secondary Firewall	192.168.2.5	255.255.255.240	192.168.2.3	eth0.700	700	DMZ Switch Secondary
Firewall cluster address	192.168.2.6	255.255.255.240				
DMZ to LAN	**192.168.2.16/28**	**255.255.255.240**			**701**	
LAN Router (Layer 3 Switch)	192.168.2.17	255.255.255.240	192.168.2.22	port 2/1 and 3/1	701	Both DMZ Switches
Primary Firewall	192.168.2.20	255.255.255.240	192.168.2.3	eth1	701	
Secondary Firewall	192.168.2.21	255.255.255.240	192.168.2.3	eth1	701	
Firewall cluster address	192.168.2.22	255.255.255.240				
WEB DMZ	**192.168.2.32/28**	**255.255.255.240**			**702**	
Primary Firewall	192.168.2.33	255.255.255.240		eth0.702	702	DMZ Switch Primary
Secondary Firewall	192.168.2.34	255.255.255.240		eth0.702	702	DMZ Switch Secondary
Firewall cluster address	192.168.2.35	255.255.255.240				
WEB Server #1	192.168.2.36	255.255.255.240	192.168.2.35		702	DMZ Switch Primary
WEB Server #2	192.168.2.37	255.255.255.240	192.168.2.35		702	DMZ Switch Secondary
Mail DMZ	**192.168.2.48/28**	**255.255.255.240**			**703**	
Primary Firewall	192.168.2.49	255.255.255.240		eth0.703	703	DMZ Switch Primary
Secondary Firewall	192.168.2.50	255.255.255.240		eth0.703	703	DMZ Switch Secondary
Firewall cluster address	192.168.2.51	255.255.255.240				
Mail Server	192.168.2.52	255.255.255.240	192.168.2.51		703	DMZ Switch Primary
DNS DMZ	**192.168.2.64/28**	**255.255.255.240**			**704**	
Primary Firewall	192.168.2.65	255.255.255.240		eth0.704	704	DMZ Switch Primary
Secondary Firewall	192.168.2.66	255.255.255.240		eth0.704	704	DMZ Switch Secondary
Firewall cluster address	192.168.2.67	255.255.255.240				
DNS Server	192.168.2.68	255.255.255.240	192.168.2.67		704	DMZ Switch Primary
Proxy DMZ	**192.168.2.80/28**	**255.255.255.240**			**705**	
Primary Firewall	192.168.2.81	255.255.255.240		eth0.705	705	DMZ Switch Primary
Secondary Firewall	192.168.2.82	255.255.255.240		eth0.705	705	DMZ Switch Secondary
Firewall cluster address	192.168.2.83	255.255.255.240				
Proxy Server	192.168.2.84	255.255.255.240	192.168.2.83		705	DMZ Switch Primary
Partners DMZ	**192.168.2.96/28**	**255.255.255.240**			**706**	
Primary Firewall	192.168.2.97	255.255.255.240		eth0.706	706	DMZ Switch Primary
Secondary Firewall	192.168.2.98	255.255.255.240		eth0.706	706	DMZ Switch Secondary
Firewall cluster address	192.168.2.99	255.255.255.240				
Partners SSH Server	192.168.2.100	255.255.255.240	192.168.2.99		706	DMZ Switch Primary
Sync between firewalls	**1.1.1.0/24**	**255.255.255.0**				
Primary Firewall	1.1.1.1	255.255.255.0		eth2		direct cross cable
Secondary Firewall	1.1.1.2	255.255.255.0		eth2		direct cross cable

External Addresses

First ISP

Hostname	IP Address	Subnet Mask	Interface
ISP A	**N.23.23.96/29**	**255.255.255.248**	
Router1	N.23.23.97	255.255.255.248	atm4/0
ISP A Router	N.23.23.98	255.255.255.248	N/A

Second ISP

Hostname	IP Address	Subnet Mask	Interface
ISP B	**M.10.172.0/29**	**255.255.255.248**	
Router2	M.10.172.1	255.255.255.248	atm4/0
ISP B Router	M.10.172.2	255.255.255.248	N/A

GIAC External Addresses (implemented by NAT on the Firewall). Whole class C distributed to ISPs via BGP

Server	IP Address	Subnet Mask	Public DNS name
External IPs of GIAC	**X.17.5.0/24**	**255.255.255.0**	
WEB Server #1	X.17.5.11	255.255.255.0	wsrv01.giac.com
WEB Server #2	X.17.5.12	255.255.255.0	wsrv02.giac.com
WEB Servers Cluster address	X.17.5.10	255.255.255.0	www.giac.com
Mail Server	X.17.5.13	255.255.255.0	mail01.giac.com
DNS Server	X.17.5.14	255.255.255.0	ex-dns01.giac.com
Proxy Server	X.17.5.15	255.255.255.0	gprx01.giac.com
Partners SSH Server	X.17.5.16	255.255.255.0	psrv01.giac.com

H/W and S/W specification for Internet gateway components

Routers connected to ISPs

Firewalls

S/W: Checkpoint Firewall-1 NG AI (R55) version. For clustering: Checkpoint ClusterXL. To improve performance and better dual CPU usage: Checkpoint SecureXL .
H/W: HP DL360 G3 (dual CPU) server with 3 NICs (strong server needed, because we are going to run WEB load balancing and RAS VPN on the same box + clustering. The bottle neck is usually CPU, this why we need real dual CPU server). Two 36GB hard drives with disk mirroring option activated
OS: Checkpoint SecurePlatform (R55)

Firewall management server (SmartCenter)

S/W & OS: Checkpoint SmartCenter on SecurePlatform (R55). It will be used as Firewall logging server as well
H/W: HP DL380 with at least four 36GB hard drives with disk mirroring option activated (one logical drive of 72GB)

IDS

H/W: HP DL360
OS: Red Hat Linux 9.0
S/W: Snort v2.1.2

Proxy

H/W: HP DL360
OS: Red Hat Linux 9.0
S/W: Squid 2.5 (stable5), TIS FWTK 2.1 (http://www.fwtk.org) package for ftp, telnet and general plug gateways, and SS5 ver 2.4 mr6 for SOCKs server (http://www.linux.org/apps/AppId_8561.html). Although no current requirement to use SOCKs protocol, this might be very useful tool for fulfilling special applications need. Every client application that should communicate with server on Internet can be socksified on the client and use this server for going to Internet.

DNS

H/W: HP DL360
OS: Red Hat Linux 9.0
S/W: Bind9

Mail

H/W: HP DL360
OS: Red Hat Linux 9.0
S/W: Postfix (http://www.postfix.org/)

Network Management Server

H/W: HP DL380
OS: Red Hat Linux 9.0
S/W: OpenNMS (http://www.opennms.org)

Linux OS Remark

Because of Red Hat end of support for standard desktop editions – according the budget constrains, the recommendation is to consider replacement of mentioned above 9.0 version with supported Enterprise WS 3.0 .

Assignment 2 – Security Policy and Component Configuration

Router connected to ISP

Objective:

- Harden the router: no extra services. Telnet and SNMP access from limited number of **internal** IP addresses. No source routing. Encrypted passwords. No ICMP replies
- Anti spoofing including "weird" addresses like 127.X.X.X, 224.X.X.X, zero addresses, direct broadcasts, …

- Because our main security and logging device is Firewall, Router ACLs will be kept as simple as possible and logging will be minimal for performance reason

Configuration:

conf t
enable secret Isp#rtr@Giac!
service password-encryption
no service tcp-small-servers
no service udp-small-servers
no ip direct-broadcast
no ip unreachables
no ip source-route
no service finger
logging 10.1.1.97
banner login # UNATHORIZED ACCESS IS PROHIBITED! #
ip access-list extended inbound_from_isp
remark * deny loopback, multicast and zero addresses**
deny icmp any any redirect
deny ip 127.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 31.255.255.255 any
deny ip host 0.0.0.0 any
remark *** deny spoofed GIAC addresses
deny ip X.17.5.0 0.0.0.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.0.0.255 any
remark * permit only ISP router communicate with the router**
permit ip N.23.23.97 0.0.0.0 N.23.23.98 0.0.0.0
deny ip N.23.23.97 0.0.0.0 any log
remark *** Allow connectivity to DMZ (security enforced by Firewall)
permit ip any X.17.5.0 0.0.0.255
deny ip any any
exit
interface atm 4/0
description *** Connection to ISP A ***
mtu 1500
ip address N.23.23.97 255.255.255.0
pvc 0/32
ip access-group inbound_from_isp in
no ip directed-broadcast
no ip redirects
ntp disable
no cdp enable
exit

LAN Layer3 switch (MSFC)

Objective

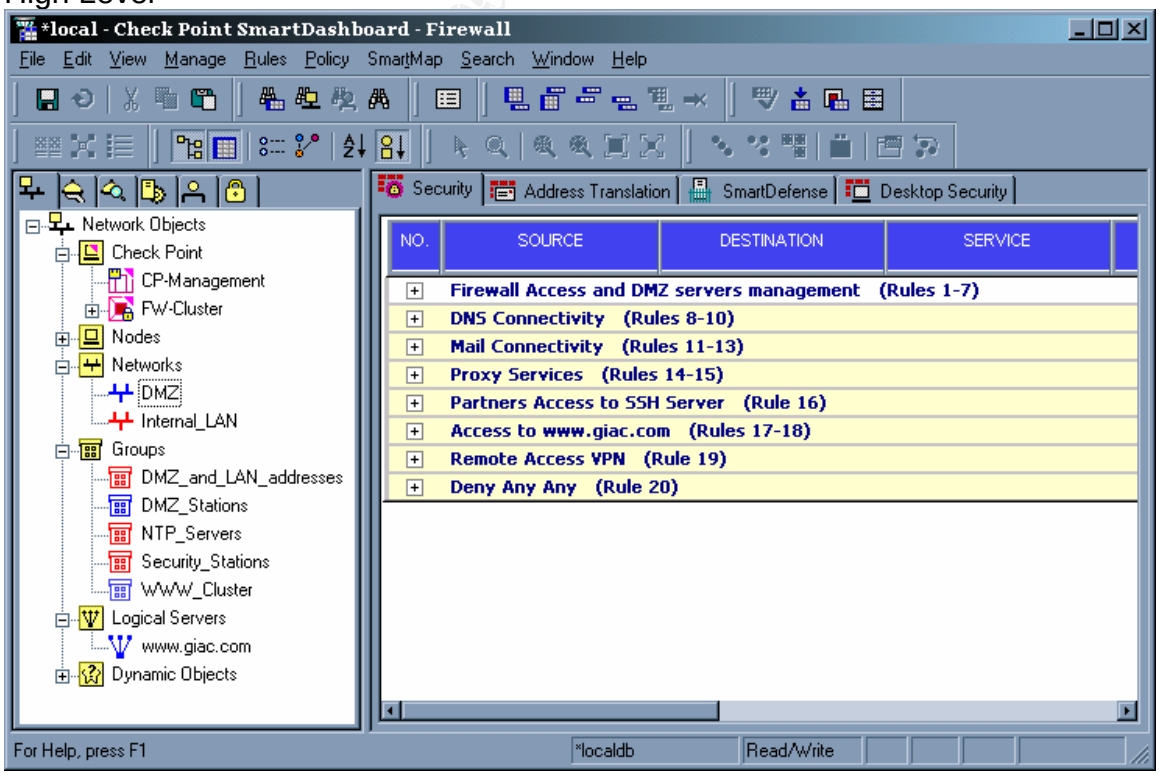
Main security objective is to limit access to SQL server that holds all the sensitive data. Will be done with ACL, allowing connectivity from WEB servers and hardened management station

Configuration

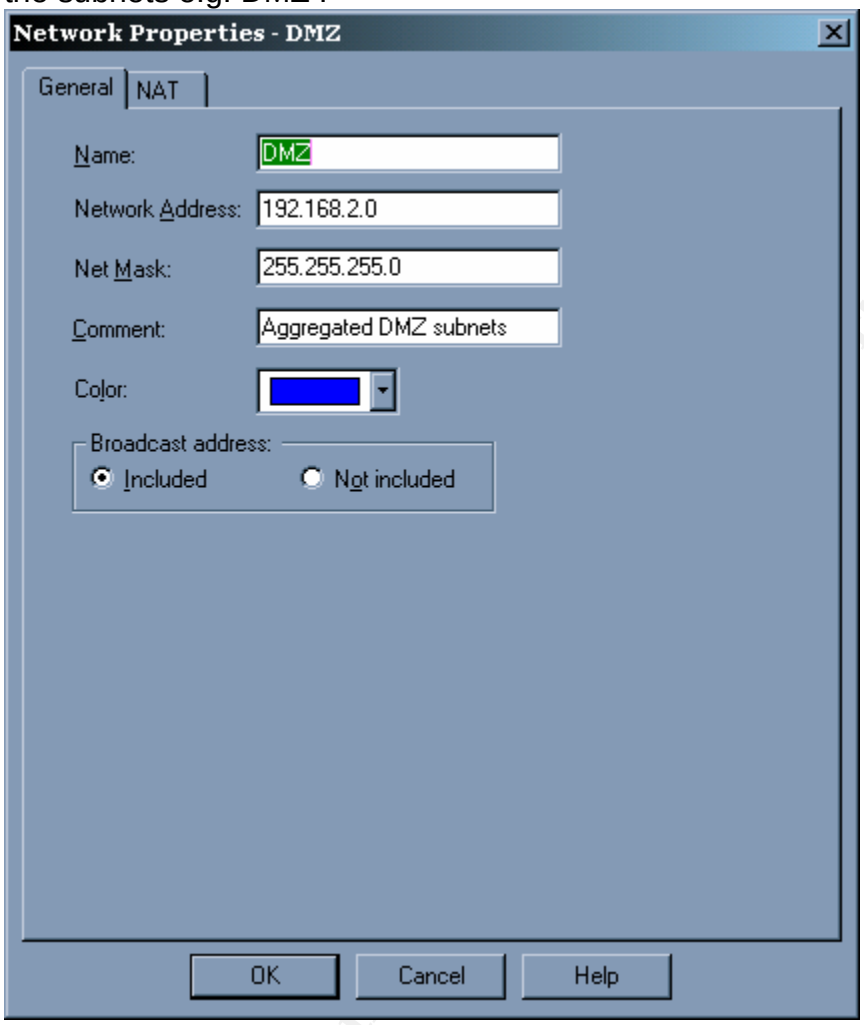
```
ip access-list extended outbound_sql_vlan
        remark *** Default 1433 port replaced on the SQL server with 9117. web
        servers (sql clients) should be configured accordingly
        permit tcp 192.168.2.36 0.0.0.0 10.1.2.17 0.0.0.0 9117
        permit tcp 192.168.2.37 0.0.0.0 10.1.2.17 0.0.0.0 9117
        remark *** DBA management station and domain controller
        permit ip 10.1.1.121 0.0.0.0 10.1.2.17 0.0.0.0
        permit ip 10.1.1.121 0.0.0.0 10.1.2.111 0.0.0.0
        deny ip any any log
Interface Vlan20
        description *** SQL Server VLAN ***
        ip address 10.1.2.1 255.255.255.0
        ip access-group outbound_sql_vlan out
```

Firewall Configuration

High Level

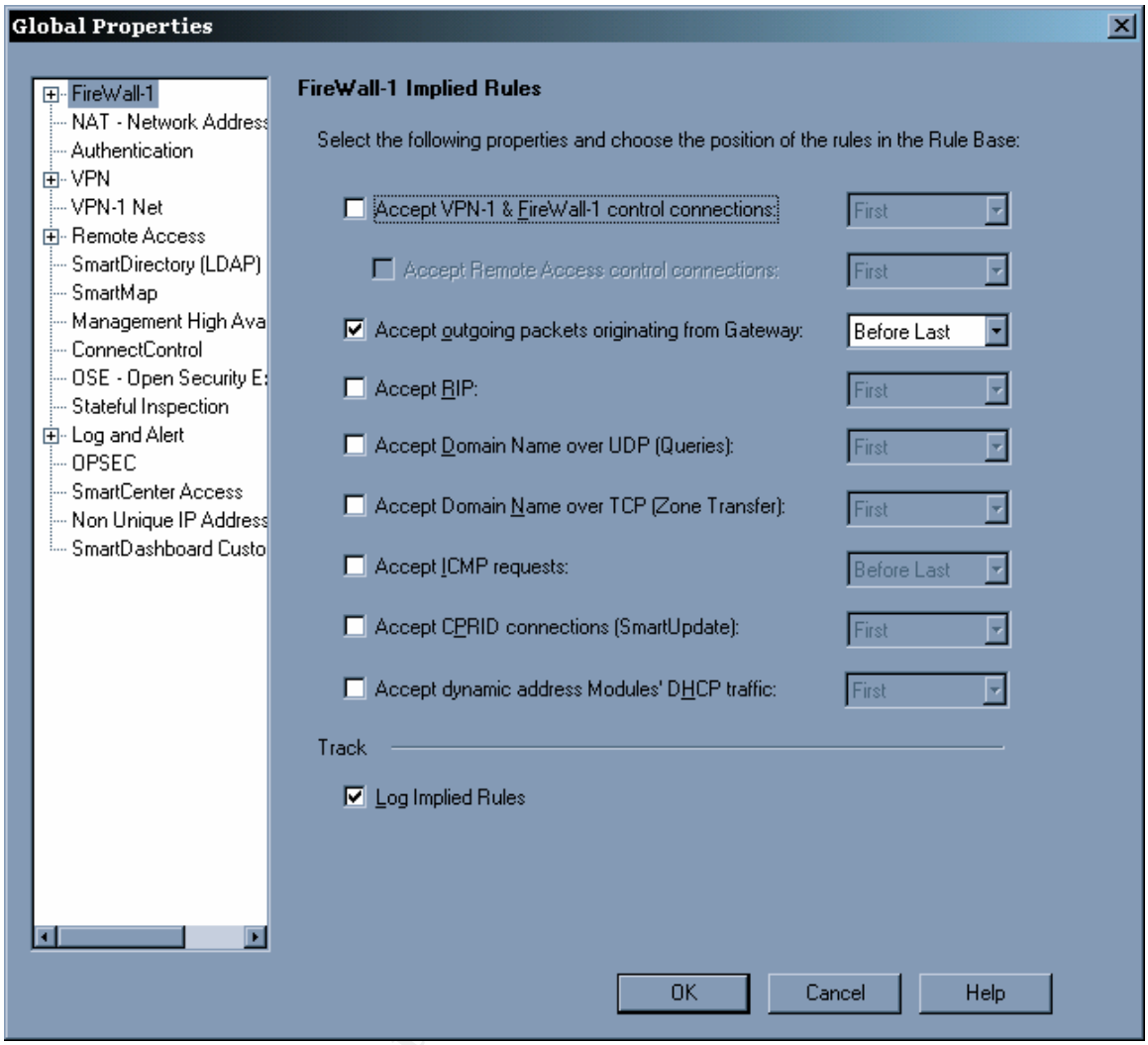


Color scheme used: LAN – Red, DMZ – Blue, Internet – Black.
For networks, instead of using Group, I used aggregated scope that covers all the subnets e.g. DMZ :



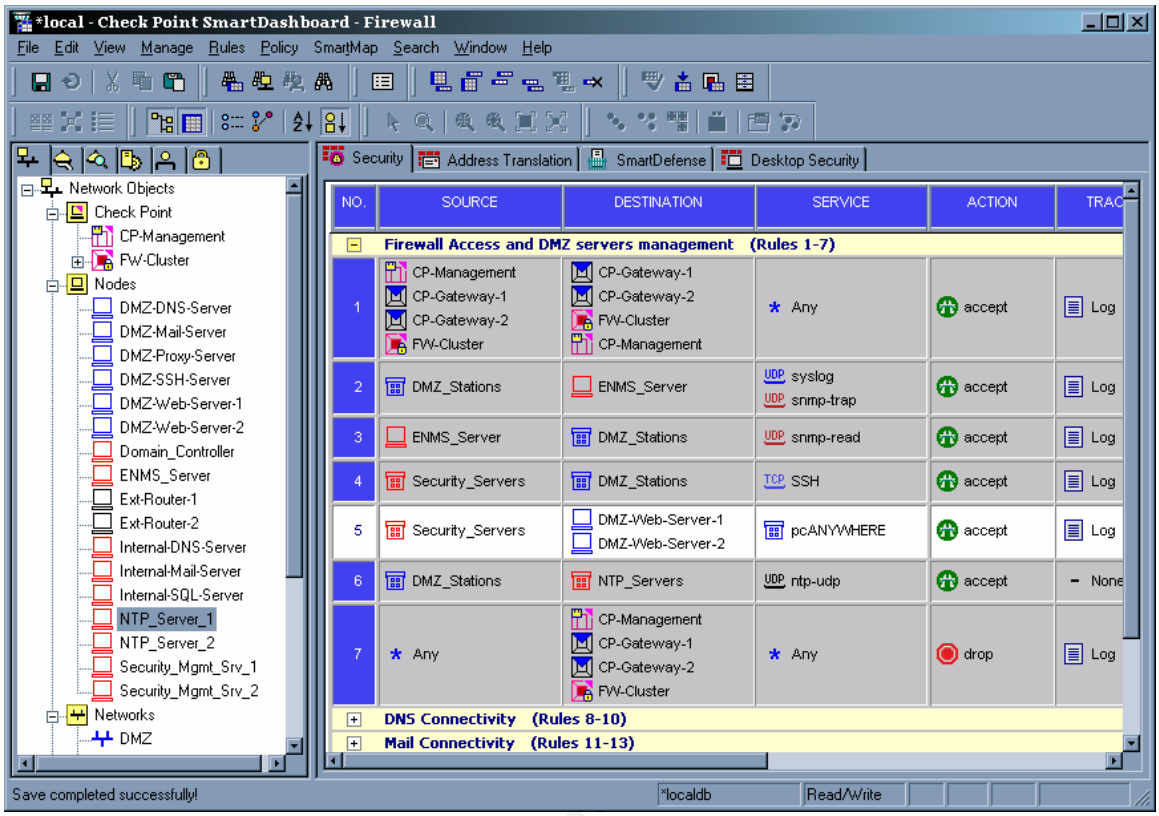
Global Properties

It is important to disable unneeded rules that are allowed by default as Implied Rules

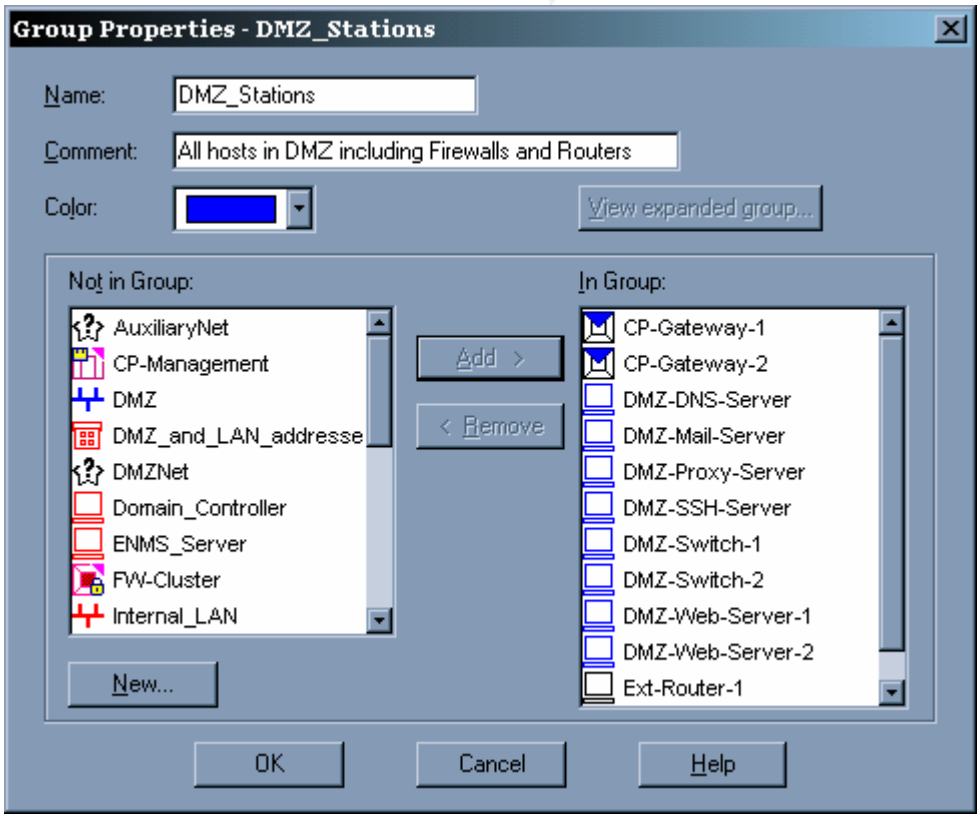


Firewall Access and DMZ servers management

Firewalls should be accessed from Management server. It is possible to reduce the services from “Any” to more specific Checkpoint protocols, but the advantage is minimal, because FWs are not listening to any other ports.
All Servers in DMZ should send alerts and syslog messages to ENMS Server.
The management of the servers and Network equipment (Switches, Routers and Firewalls) in DMZ should be done via SSH only and from limited number of hosts on the LAN (Security_Servers group).
The exceptional are Windows IIS Servers that will be managed remotely with pcAnywhere also from limited number of LAN stations.
To manage DMZ equipment from home, Remote Access VPN must be established first (see RAS VPN Access rules). The rule will allow connection to LAN Security_Servers after VPN establishment.
For log analysis, it is highly valuable to sync all the equipment clocks. Rule #6 allowing connection to two NTP servers in LAN

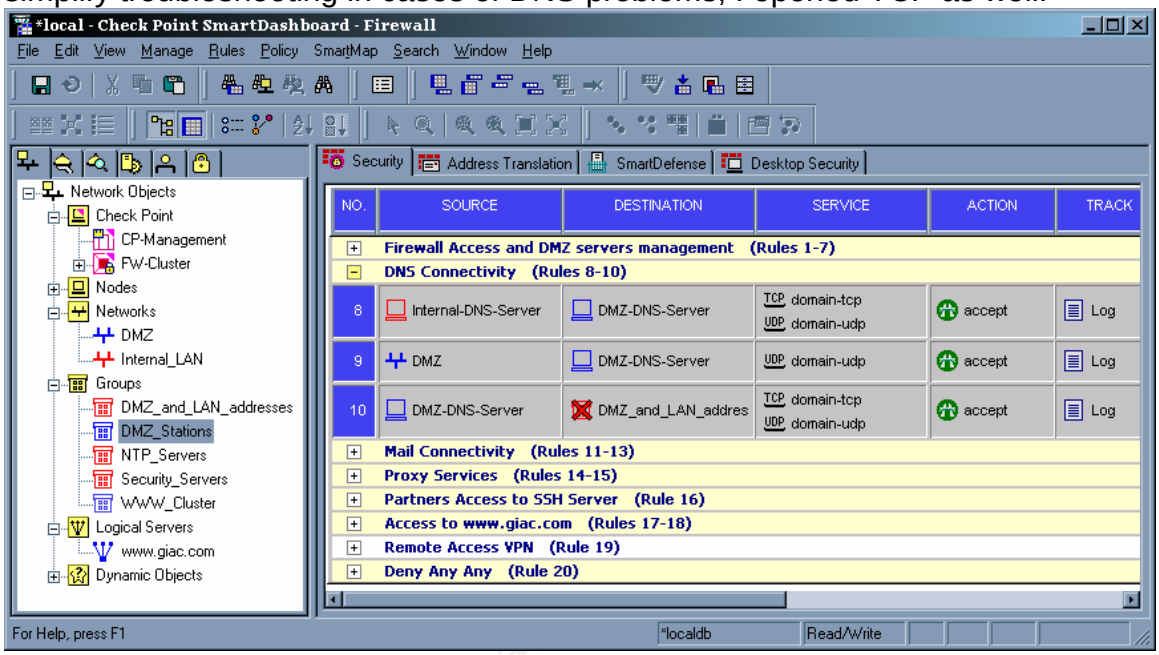


DMZ_Stations are all hosts in DMZ including Routers connected to ISP, DMZ Switches and Firewalls:

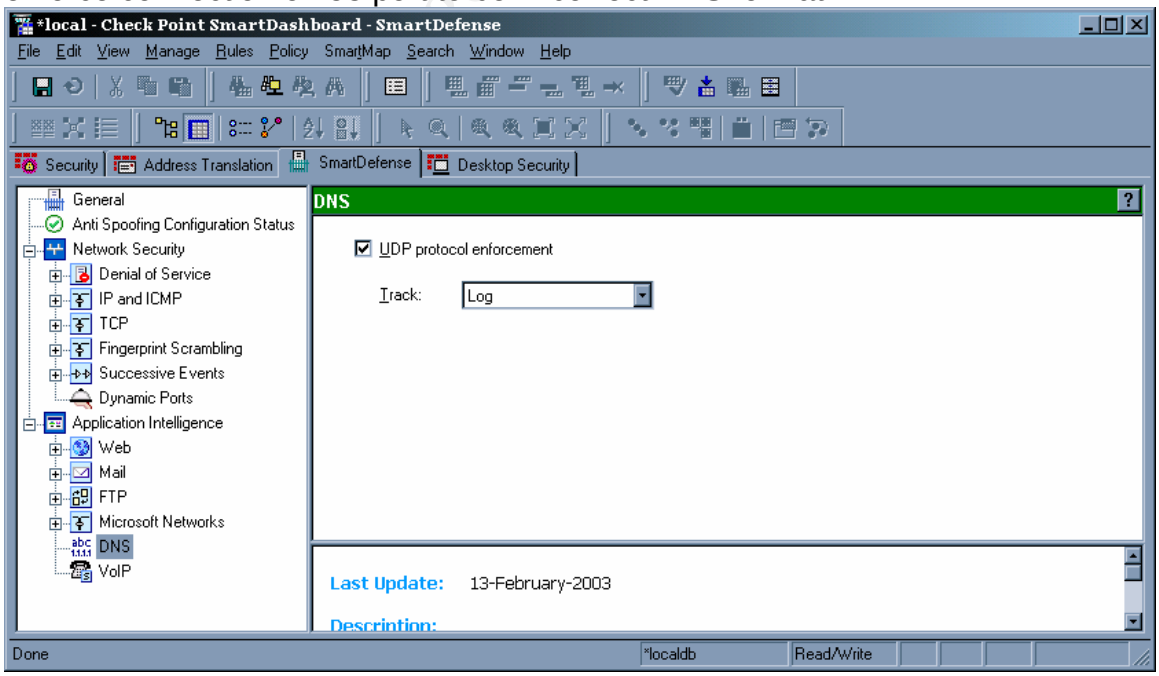


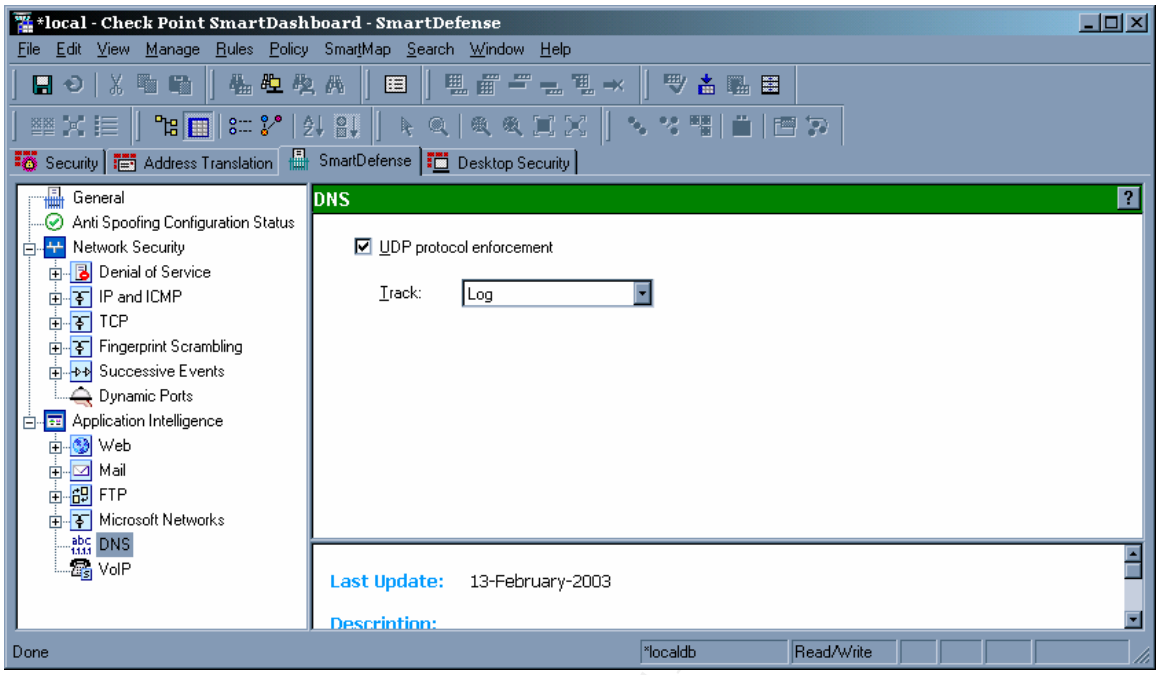
DNS Connectivity

DNS server in DMZ serves hosts in DMZ and as “relay” for LAN (internal) DNS server to resolve names on Internet. It also acts as authority for Giac DMZ servers. No internal DNS info should be exposed to Internet. TCP is used for zone transfers and if answer to DNS is longer then 1.5Kb . Probably only UDP to Internet would be sufficient, but the risk of outbound requests is very low, so to simplify troubleshooting in cases of DNS problems, I opened TCP as well.



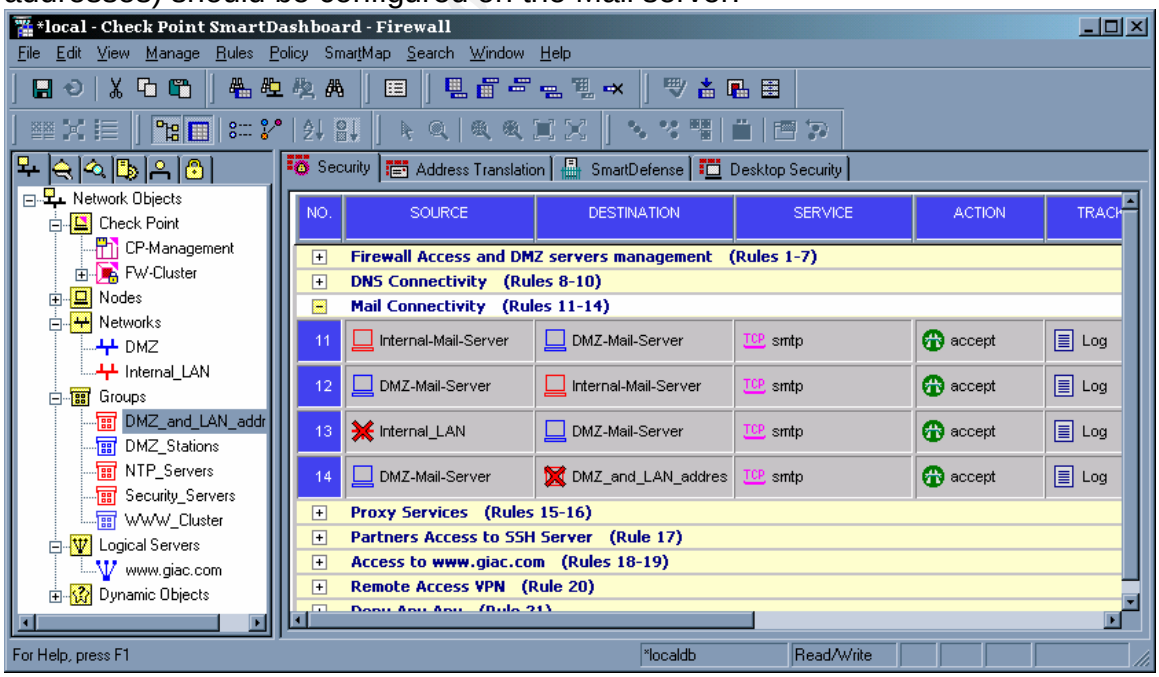
Additional DNS security should be configured with SmartDefense. This will enforce connection on 53 port to be in correct DNS format.



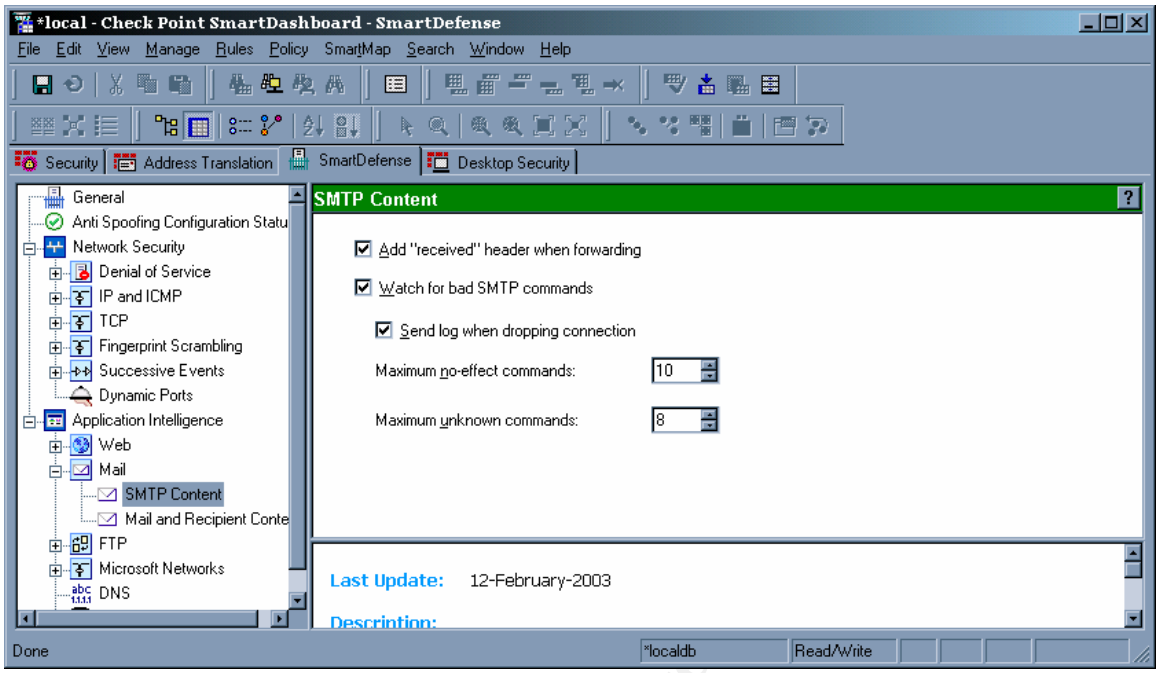


Mail Connectivity

DMZ Mail relay, should accept smtp connections from Internet, Internal Exchange Server and DMZ servers. It should send mails to Internet and to Internal Exchange server. Protection of the mail server not to act as relay for Spammers (mails from Internet can be addressed only to Internal Giac addresses) should be configured on the Mail server.

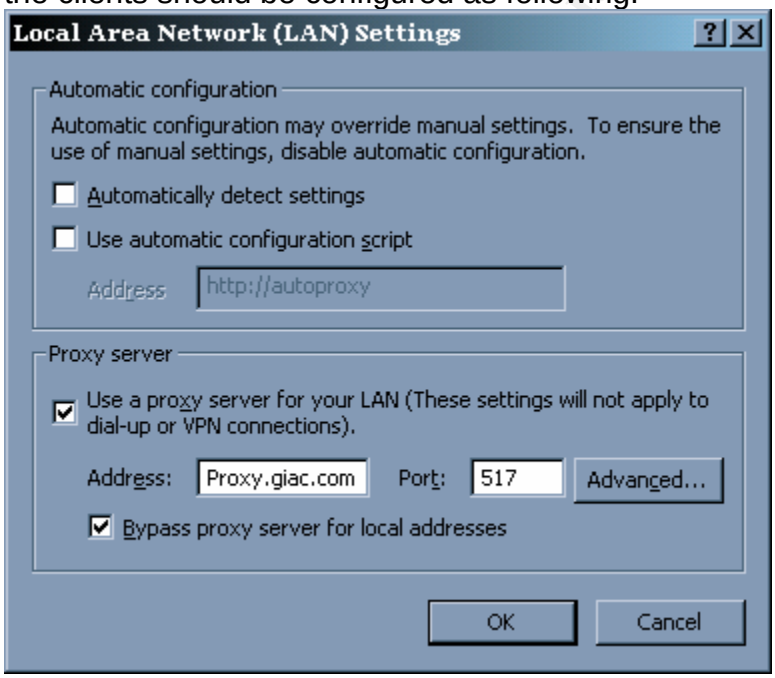


Additional SMTP protection should be configured with SmartDefense. It will mainly enforce RFE compliance with SMTP protocol

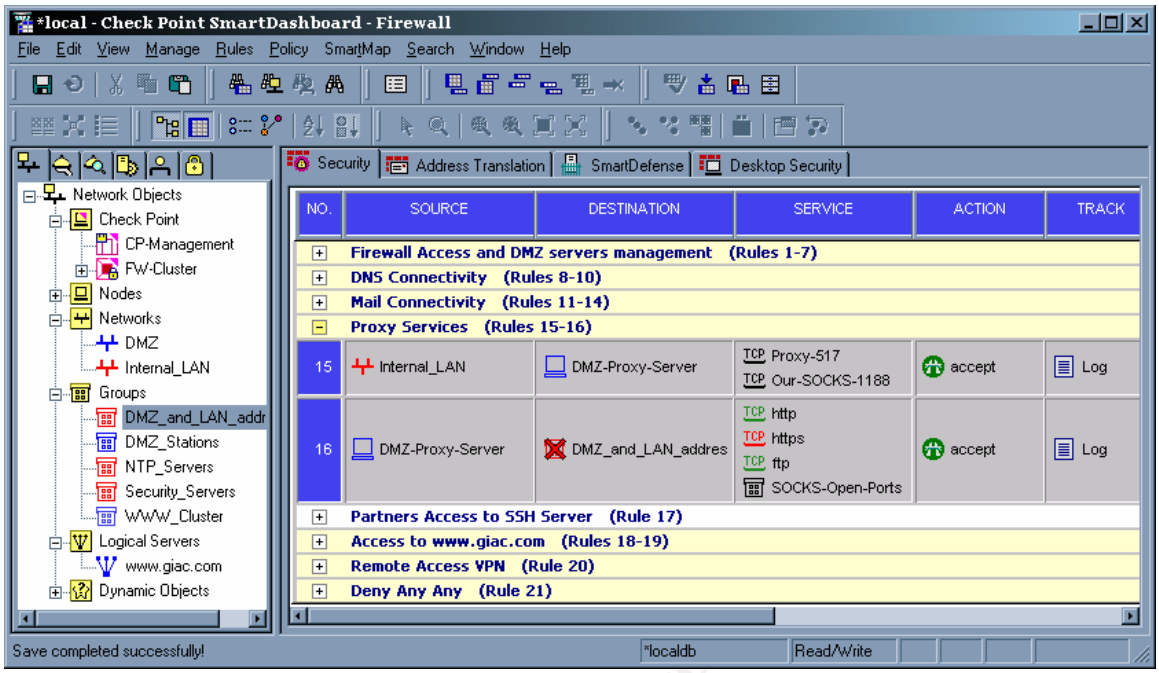


Proxy Services

All internal users should use Proxy to get to the Internet. The Internet browser of the clients should be configured as following:

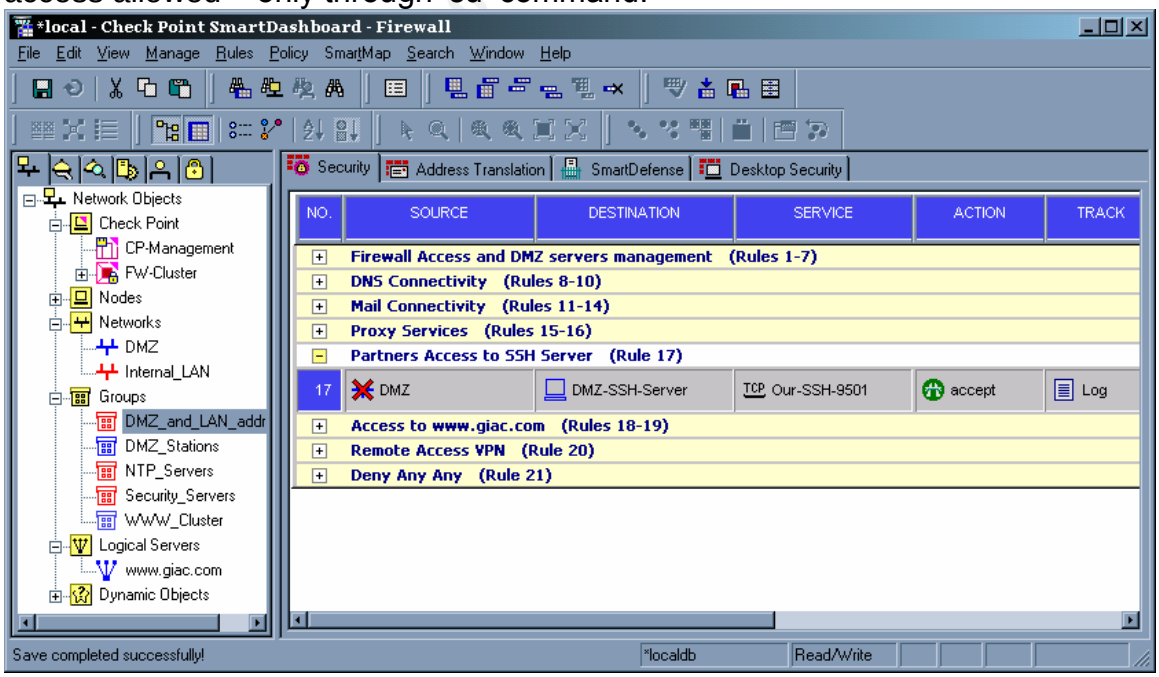


The Proxy server is also used for ftp connections. SOCKS proxy is running on the server as well - listening on 1188 port (not standard 1080). Each open port for outgoing connection should be also updated in the Firewall under [SOCKS-Open-Ports] group.



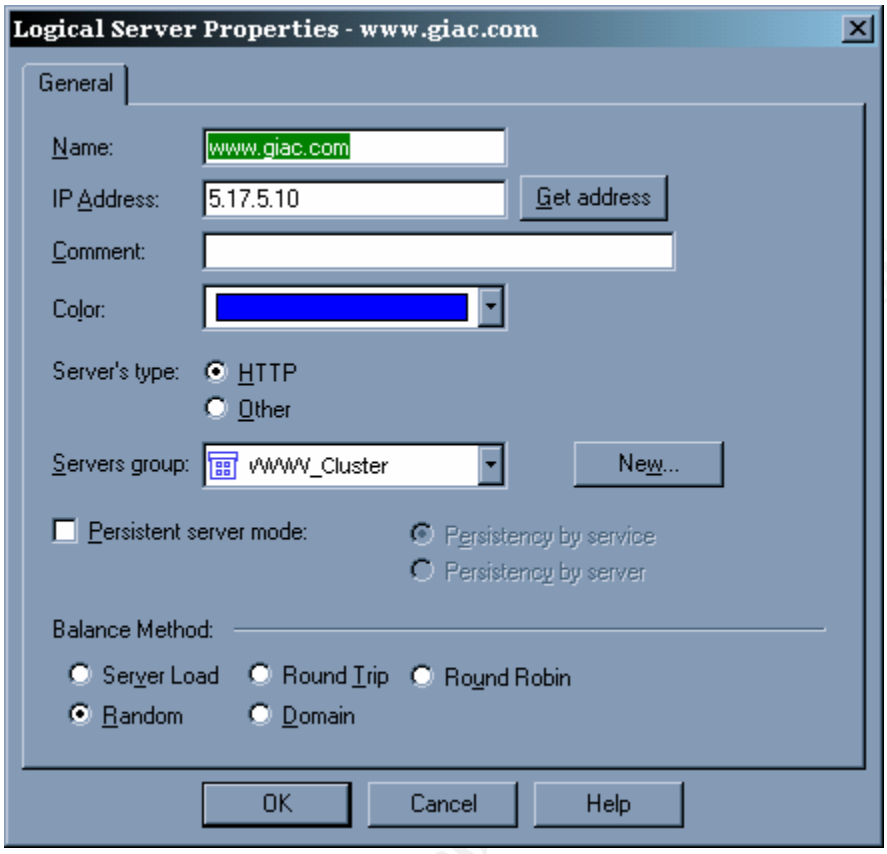
Partners Access to SSH Server

As stated, there is SSH server in DMZ for partners to upload the sayings. SSH server should be configured to listen on non standard 22 port (9501 in our case). LAN and Internet users can access the server. No connections from the server allowed, so if it will be compromised, no further access is allowed. On the servers accounts for partners and Giac users should be configured appropriately. No root access allowed – only through 'su' command.

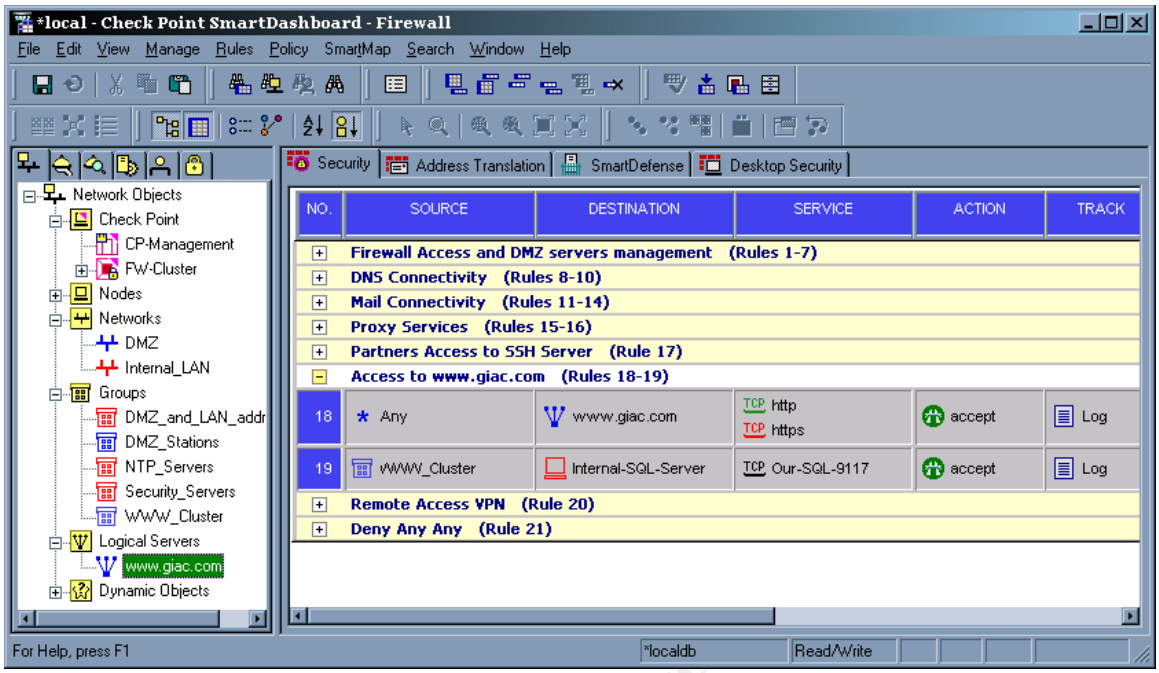


Access to www.giac.com

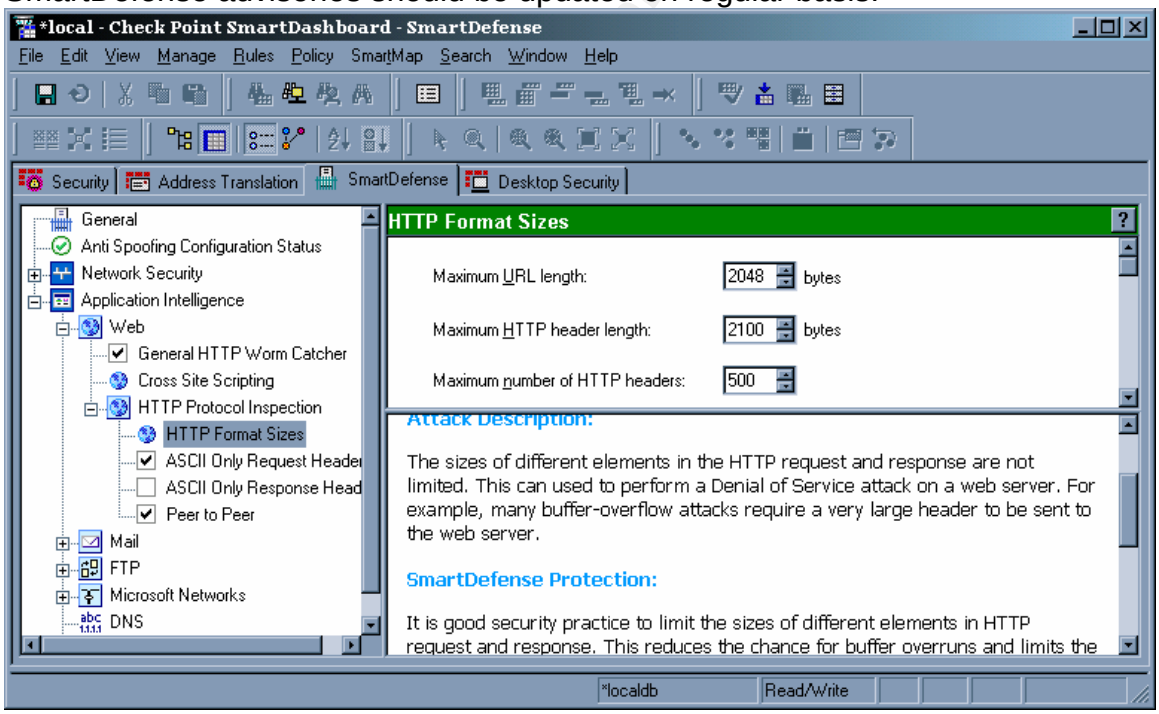
Logical server for cluster address configured to make load balancing between the two web servers



Both web servers need to access the internal SQL server. The SQL server should be configured to listen on non standard 1433 port - 9117 in our case. The assumption that the applications running on the web servers can easily be updated with new connection string adding/replacing existing port to 9117. In very rear situation that because of some reason the applications can not be updated, the [Our-SQL-9117] port should be replaced with standard [TCP-1433]



Additional security should be configured with SmartDefense. Checkpoint SmartDefense advisories should be updated on regular basis.

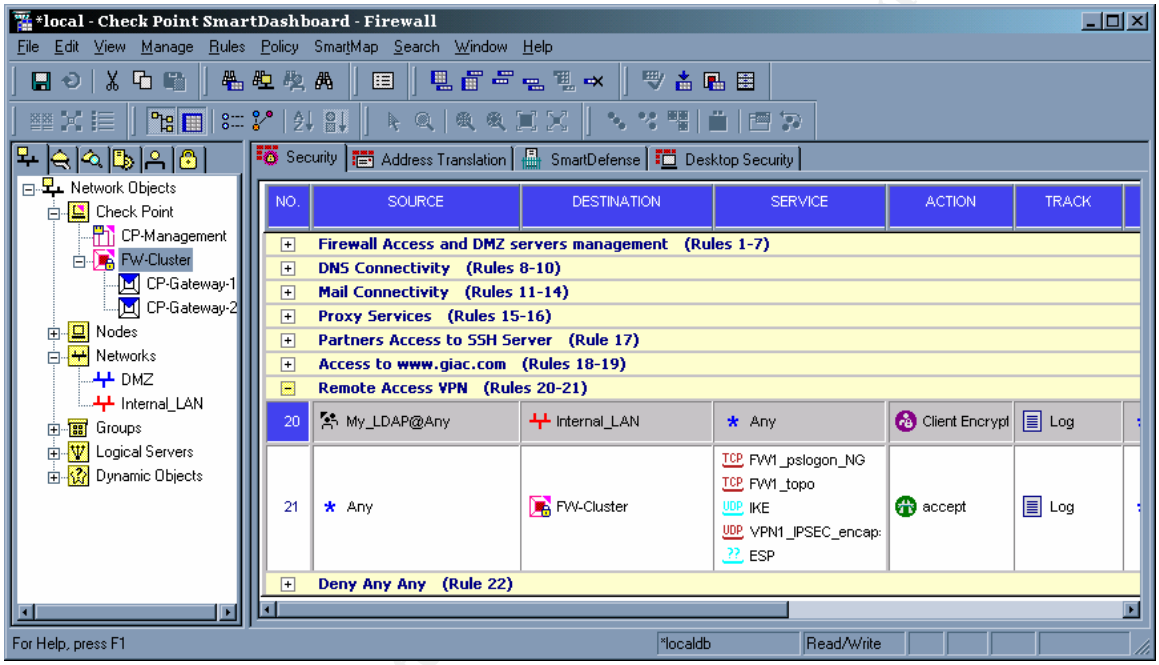


Probably the URL length can be even reduced more – however 2K is usually will not cause Buffer Overflow and sometimes URLs do consists of big number of parameters (we don't want our users to complain that they can not access some sites on Internet…)

Remote Access VPN

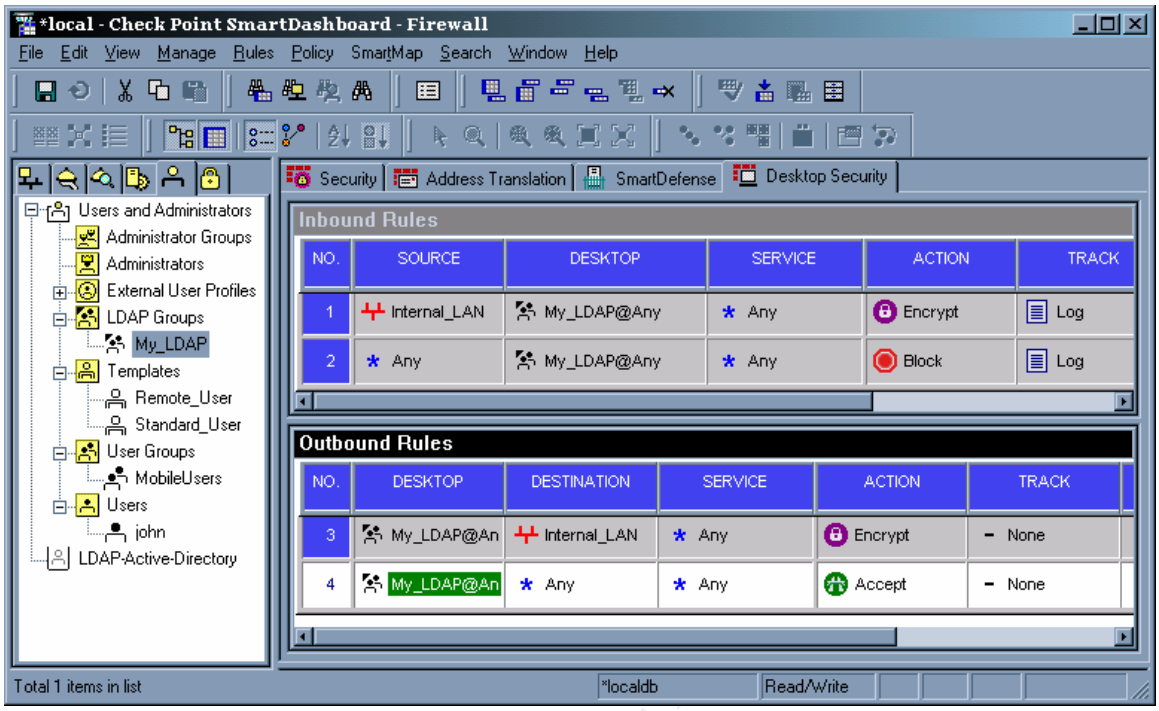
Checkpoint SecureRemote client should be installed on the notebooks. In SmartDashboard under [Global Properties] set Encryption Algorithm to AES-128 and for IKE use Diffie-Hellman group 2 (1024 bit). Leave all the other at default values.
The users authentication will be done with Microsoft Active Directory. Inbound connection to the Secureremote while connected through VPN will be restricted from LAN addresses only.

The rule in for the VPN access



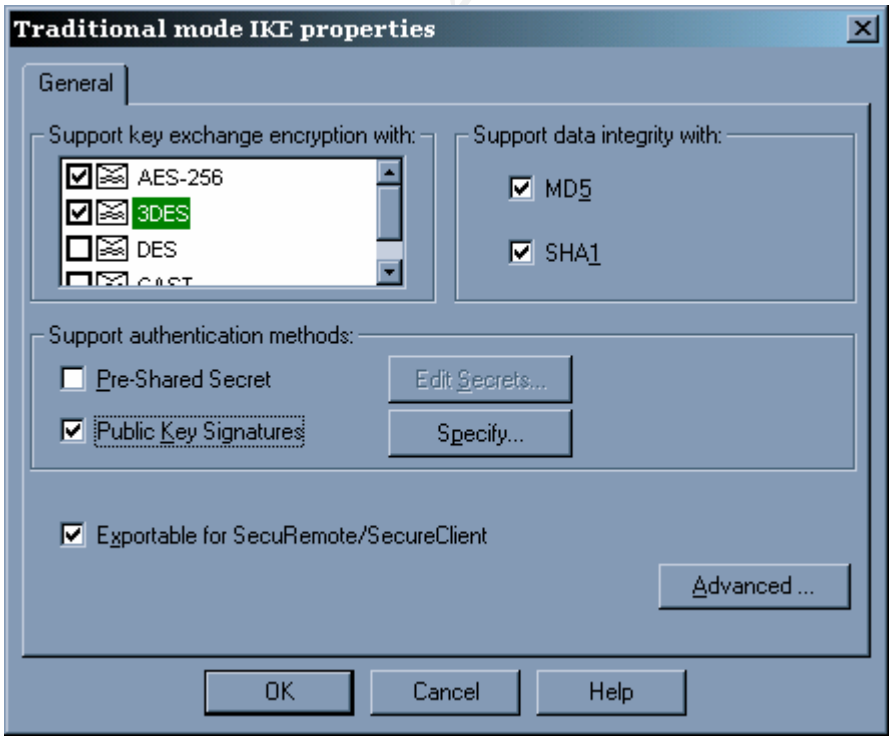
Rule #20 permits remote users to access LAN. Rule #21 allows to establish encrypted session with the Firewall and fetch the security policy (FW1 services)

Secure Desktop rules to be fetched by the client

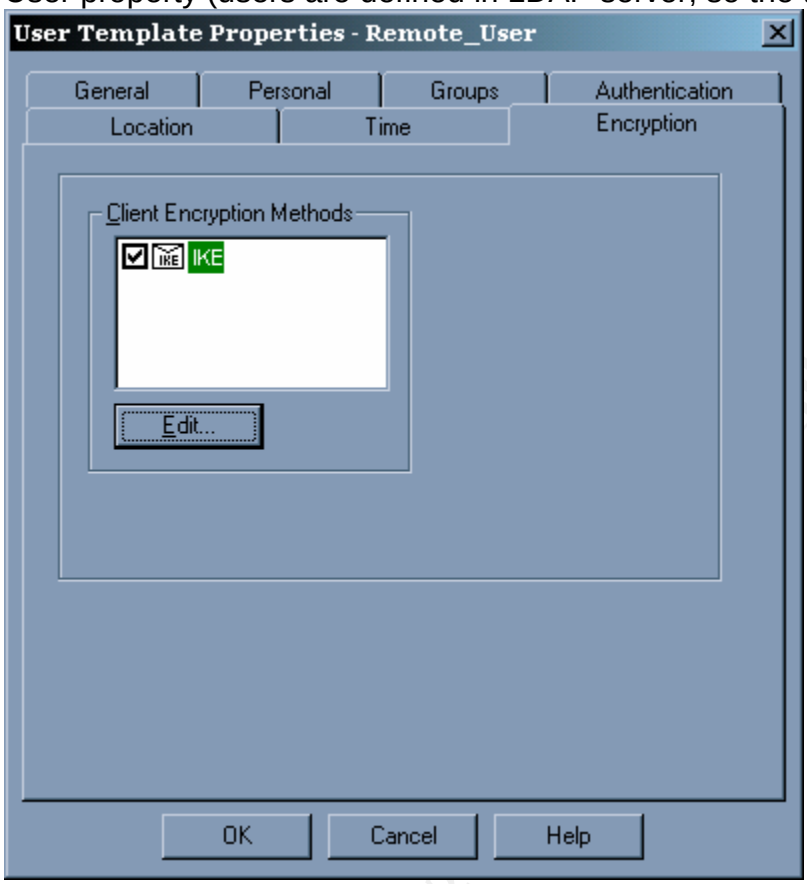


While not connected to LAN, I would like to allow users browse freely the Internet and I don't want to log their sessions (so they will feel comfortable). However inbound traffic must be tightly restricted and logged to identify connections attempts.

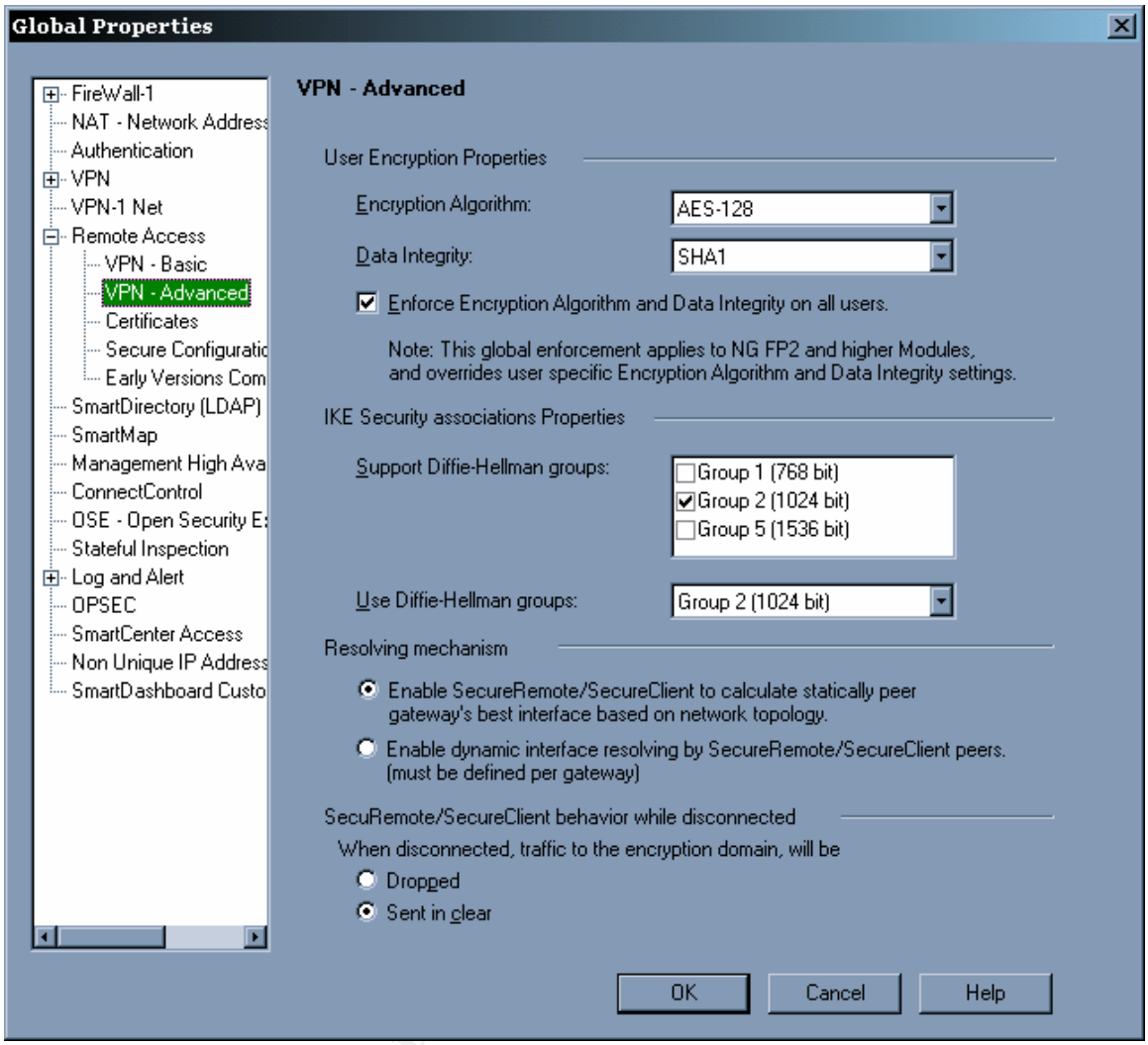
Firewall properties (under gateway object) for VPN connection with SecureRemote:



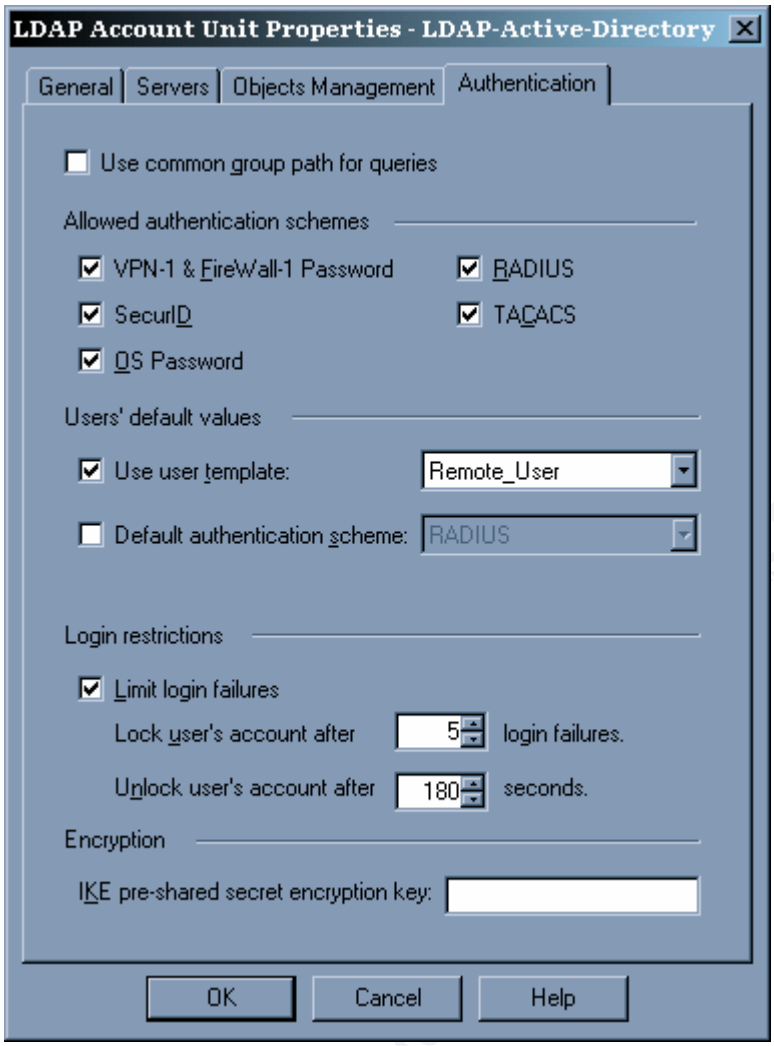
User property (users are defined in LDAP server, so the template is needed)



Global Properties for encryption parameters



LDAP Server

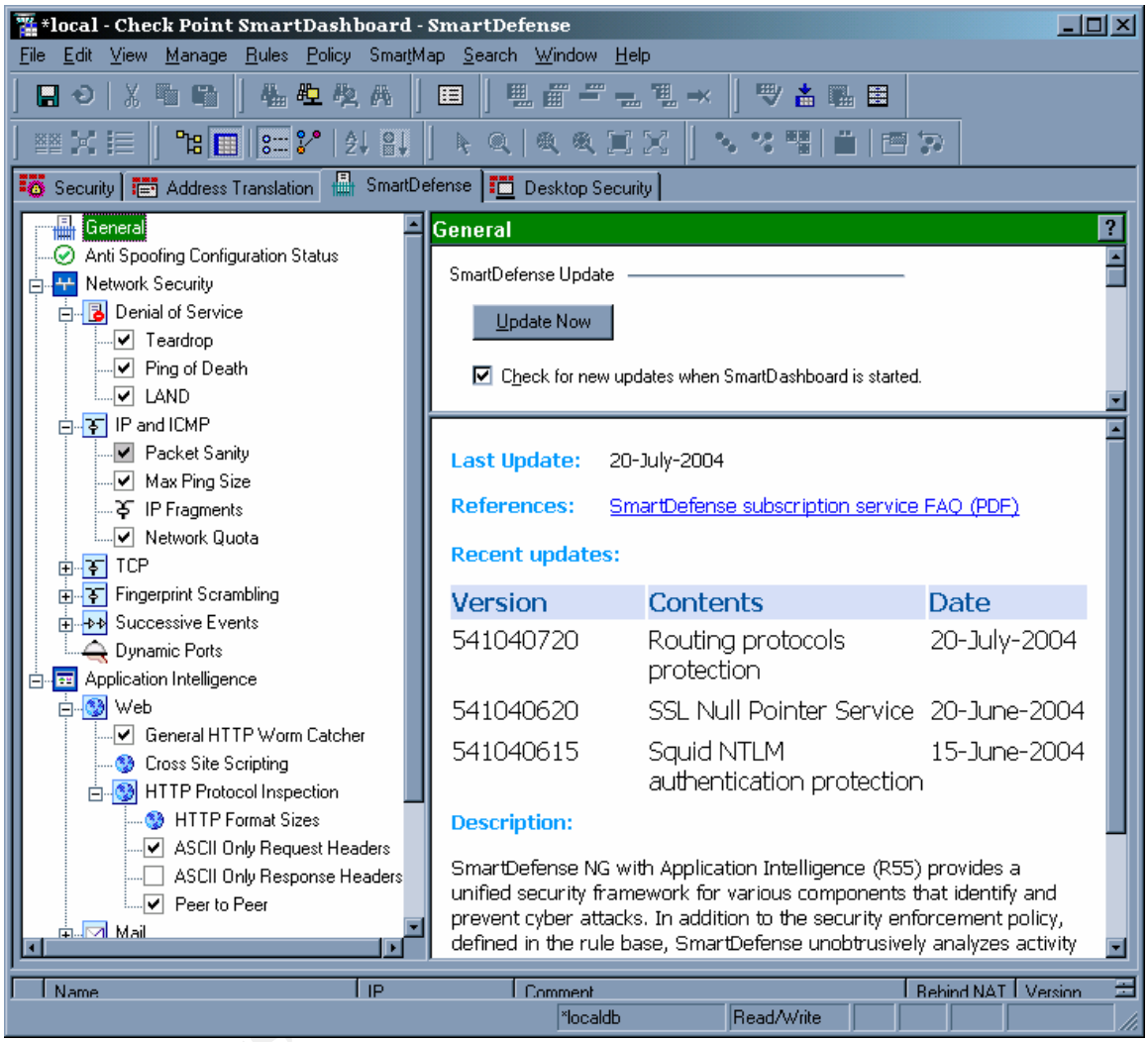


VPN users are granted for full access to the LAN. It will be management nightmare to allow Remote Access per protocol/destination.
Because this is probably the weakest link in the perimeter security (because of notebook exposure to Internet, home WLAN, public hot spots, shared cable networks, notebook steal …) special attention should be done on the IDS and log analysis of the VPN users IP scope. All remote users must have automatic antivirus update enabled. Checkpoint suggests capability of identifying patch versions (from registry) before allowing connection. This option should be seriously considered.

SmartDefense

SmartDefense is new Checkpoint additional capability to identify some of Layer3 up to Layer7 (for number of specific protocols) attacks. For “security in depth” reason we will activate the main options especially protection from “ping of death”, “syn” attacks and general http worm catcher. To get advisories/patches

how to block new vulnerabilities special subscription should be purchased from Checkpoint.
Some of the Layer 7 inspections can make a hit on the FW performance. So I will not suggest activating all the options e.g. for FTP that is used through proxy only.



Assignment 3 – Design Under Fire

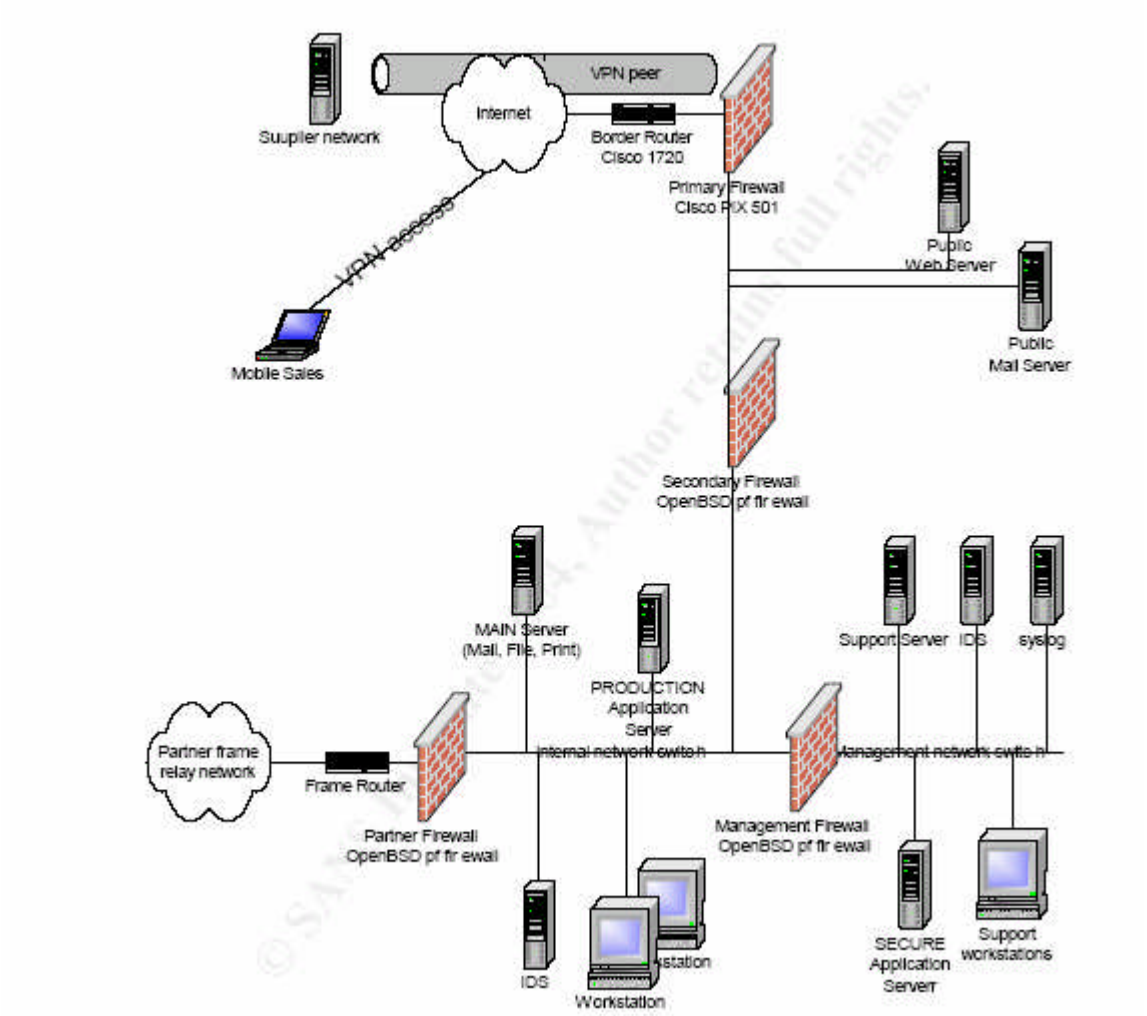
Attack Options Overview

I will describe attack performed on the design made by Marc Panet-Raymond on March 1, 2004
Citation from this work will be used in quotes and in blue color e.g. “Rune Enterprises is a small family business specializing in providing proverbs enhanced by Rune magic” [page #2]

The target of an attack is “Secure Application Server” where Rune Enterprises main intellectual property is stored – “Family members take proverbs purchased

from their suppliers and enhance them using magic passed on from generation to generation. This process is done on the “Secure application server.” “ [page #3].

The design of Rune network:



The weakest link in Marc perimeter design, in my point of view, is lack of Proxy servers in DMZ. Thus connections on ports for http, https and dns are allowed “employees will have internet access with the following protocols: http, https, smtp, dns(udp)” [page # 5]. Such design however reduce number of servers that are listening to ports from internet, but simplifies much the communication with Internet once Trojan or backdoor is installed on Internal host. The design is not using internal DNS server, but uses ISP servers for name resolution. It is potential high risk, if ISP DNS administrator decides to perform the attack (or DNS server was compromised). Another weakness is lack of IDS server in DMZ, which might allow easier scanning of WEB servers for vulnerabilities.

Usually the weakest links in Corp perimeter are remote access users and partners. I can not make assumptions regarding security of partners network, but it is possible that design/detection/patching of the partner will be on much lower

level than Rune Enterprises are. Partners have access to "Production Application Server" which communicates with "Secure Application Server" that is our final goal of the attack. This direction might be very promising, but I will not go into this option, because lack of data on Partners Network design & security.

The most promising option is penetrate to the LAN through Remote Access VPN users. According the design they are not using certificates or SoftID – "Each sales person has their own password to access the VPN since they are not numerous" [page 5]. And on page 35 – "Since this Rune Enterprises is small company we do not use the certificate for
VPN connections due to their complexity at this time"
Thus it is possible to connect from any computer on the Internet if you know the user name and password.

The following options might be used for attack:

Option	Method	Caveats
Via Partner	• Compromise Partner • Connect to Production Application Server • From the server continue attack on the LAN hosts	Partner network might be secured not less than Rune network
Via ISP DNS	• Get administrator privileges on ISP Server • Change IP of one of the sites accessed by Rune users with my own • Download malicious ActiveX as soon someone from Rune connects (redirect to real site for all others) • From this client continue attack on the LAN hosts	Need administrator access to ISP DNS. Might be very easy if I am ISP employee or can insert myself as man in the middle (not encrypted UDP traffic). Otherwise requires attack on the DNS server e.g. cache poisoning.
Via WEB server	• Exploit Web server vulnerabilities • From the server continue attack on the LAN hosts	Requires be one step ahead Rune administrators as soon vulnerability for Linux, Apache, MySQL, OpenSSH, OpenSSL is detected.
Remote Users	• Install Trojan on Remote user's laptop	Most promising action that will be described

	• From the client continue attack on the LAN hosts	below

Attack on Remote user

High level attacking plan:

- **Find sales persons e-mail addresses**
- **Install Trojan on their laptops via malicious e-mail and get VPN password**
- **Connect to LAN through VPN**
- **Perform standard scanning for vulnerable hosts, get/sniff password files and crack them**
- **Connect to one of the LAN servers**
- **Escalate privileges to Administrator and install Backdoor**
- **Grab Password Hashes from the server and crack them**
- **Map the Network to identify location of the "Secure Application Server" (eventually will be found behind internal Firewall)**
- **Map hosts behind internal Firewall**
- **Take control of system behind the Internal Firewall**
- **Take control of Secure Application Server**
- **Steal the Rune secret from the server ("magic passed on from generation to generation" [page 3])**
-

Finding remote access (sales persons) users

There are couples of possible way to identify rune.com users. Usually companies have the standard way to assign e-mail addresses, for example first letter of the first name and then last name. The easiest way is to search with Google mailing lists for *@rune.com users. We are looking for sales persons that are connecting to the company through VPN. From Rune web site, there is a good chance to find them from "contact us" link. If not we can pretend as potential buyer and will ask from sales person to contact us. We can simple make a call to marketing of Rune and ask for sales person to make business. Finding this information through partners is also possible.
One of the ways will give us e-mail address of at least one of the travel sales person and potentially more.

Installing Trojan and Backdoor on remote access user

After I have an e-mail address I will send a spoofed mail (coming from one of the Rune customers for example) with Backdoor S/W attached to it. Usually sales persons are not IT geeks and not very cautious with opening attachments. I will masquerade the attachment within some movie or presentation with wrapper program like SilkRope (www.netninja.com/bo/index.html) or SaranWrap. Opening the attachment will show the movie and in parallel install our Trojan & backdoor application.

Other option (if the first will not work for some reason) will send mail with "please check the following web site" message. The web site will be ours (on some compromised host on the Internet) and will send to user ActiveX control including the Trojan horse application.

Because - "The VPN client is configured with no split horizon, that is when connected to
the internal network their other network connection is disabled" [page #5], we can not use the standard backdoor to listen on high port. However Internet access is allowed for rune users "employees will have internet access with the following protocols: http, https, smtp, dns(udp)" [page # 5]. And no proxies are used – so port 80 is opened from LAN.

I will use two methods:

- backdoor that makes connection over HTTP (e.g. Reverse WWW Shell or HTTPTunnel or stunnel).
- Because our goal is to get VPN password of the user, we can use Trojan that will send an e-mail to us with sniffed passwords (e-mail address will be some hotmail box created and viewed from compromised computer). Sniff passwords can be done with L0phtCrack. Additional extremely valuable method can be simply log all the user keystrokes that eventually will record the VPN password as well (built in capability in BO2K)

In Marc Panet work, the antivirus protection process is not mentioned at all. If there is no enforcement of antivirus software update on notebooks of sales persons, most of the chances that it will not be updated with last signatures.
I intend to use BO2K (www.bo2k.com) as the Trojan horse and Reverse WWW Shell (http://www.thc.org) as backdoor. To be sure that the installed s/w will not be detected by Antivirus, we must test it in the Lab. Because BO2K is coming with developer's kit, it is possible to modify it till antivirus will not recognize the Trojan. (Other option is that my program will first try to kill Antivirus process and/or change its registry settings, but the chance that Antivirus will recognize modified BO2K is very low).

Getting the VPN password and connecting to Rune LAN

I will use two ways to get VPN password:
1. Use [Key Logging] -> [Log Keystrokes] BO2K option. This capability allows to store in the local file keys typed into each window. To backup my backdoor option (if backdoor option will not work because of some policy applied on proxy or Firewall), the Trojan will add scheduled task that will mail this file to my e-mail account every 12 hours.
2. Use [System] -> [List Passwords] BO2K option to gather passwords from the sales person laptop. In most cases standard users (like sales persons) use the same password for company related access. The list of password hashes got from the computer, we can break with L0phtCrack

As soon we have the VPN password, it is safe to make VPN connection to Rune Enterprises. The connection will be done from some compromised home PC on the Internet. This will ensure that track me back, will be extremely difficult.

The only caveat is to ensure that the sales person is not connected to VPN as well. When sales person connects to Internet, he should first get IP address from ISP provider and only then he will be able to start VPN communication. My Trojan must have a capability to send me ICMP/UDP message as soon the victim computer connects to Internet (and before establishing VPN tunnel). There is couple of existing plug-ins to BO2K that actually can do it http://prdownloads.sourceforge.net/bo2k/srv_rattler_3-03.zip will send e-mail each time it detects an IP address addition/modification (almost real time) and sending information via IRC - http://prdownloads.sourceforge.net/bo2k/srv_ricq_3-02.zip (real time).

Taking control over LAN Servers

Sales persons have access to production application server : "Access is required to the sales system on the production application server and main server" [page #5] . Production application server and main server specs are:

Main Server

The Main server has the following configuration.

- Compaq Proliant 1600
- Windows 2000 Server – SP4, patched
- Exchange 2000 – SP3, patched

Production Application Server

The Production application server has the following configuration.

- Compaq Proliant 1600
- Linux Redhat 9.0 hardened and fully patched
- Apache 2.0.48
- Tripwire, version 2.3.1-14
- Openssh, version 3.7.1p1
- Openssl, version 0.9.6l
- mysql, version 4.0
- iptables

After establishing VPN connection, I will get address from the LAN scope "VPN network – sales 192.168.10.192/28" [page # 12] . This IP will allow me full connectivity to the Servers and workstations on Internal network. "Main server" is Windows2000 server used as file share, exchange, and print server. It is the easiest target, however the Linux WEB server with mysql and openssl, can be a good target for vulnerability scanning as well.
My Trojan actually already got the sales person NT password from previous attempt to get all his passwords (sniffing passwords and/or record all keystrokes). So I can connect (map drive) to the Print server with sales person user name (net use Z: *server_name**share_name* * /USER:*username*) .

After this connection, I need to escalate privileges to administrator level. It can be done with bugtraq ID 1535 vulnerability – "Microsoft Windows 2000 Named Pipes Predictability Vulnerability". The exploit of this vulnerability can be done with PipeUpAdmin (http://www.dogmile.com).
You need to copy the software to the server and simple run from command line C:>pipeupadmin . This will add your user (you connect with) to administrators group

Grabbing SAM (getting users password list)

To get SAM file with all user's hashes, I will use Pwdump (http://razor.bindview.com). The command is:
PWDUMP3 *server_name output_file*.
This program grabs password hashes from Windows NT/2000 machines and prints them to the output_file in standard L0phtcrack format.
Cracking the hashes will give me complete list of Rune users (all users are printing and sending e-mails) with their Windows passwords. I will also install Reverse HTTP backdoor on the Main server to allow me convenient connection anytime. The connection will be done from compromised home PC on the Internet.
At this point I have a server in Rune LAN with backdoor and bunch of NT passwords that will allow me to continue the attack.

Mapping the Network

The final target is Application Server that is located behind Internal Firewall. My first task will be to map the network. To find all the hosts on the same LAN is very easy task. We can use NMapWin or SuperScan for active scanning or if we have time more secure to use sniffers. I will download to my server dsniff for Win32 (http://www.datanerds.net/~mike/dsniff.html) and NMApWin (http://www.nmapwin.org) for that task. As well for fast capture I will download WinDump. (http://windump.polito.it) .
From analyzing mac addresses from WinDump output (C:>windump), I can immediately identify that our server is connected to Switch. In Switch environment all the traffic that can be seen are broadcasts, multicasts and traffic designated to my system.
Analyzing WinDump files, I realize that bunch of IPs from 192.168.3.0/24 subnet are connecting to Main server although NMapWin can not identified them. I assume that this subnet is behind some Firewall/Router wit ACLs. I can assume as well that Secure Application Server that I am looking for is on that subnet.

To summarize the status:

1. Secure Application Server is not on the subnet(s) that can be reached directly
2. My hacked "Main Server" connects to the Switch
3. I guess that "Secure Application Server" is on 192.168.3.0/24 subnet behind Firewall or Router wit ACLs

4. I have dsniff and Windump on “Main Server” with open backdoor through Reverse WWW Shell
5. I have cracked SAM file that allows me to connect to most (or all) of Windows systems

I have the following options to continue:

Option	Method	Caveats
Sniff Network administrator password as he/she connects to Network equipment/Firewalls	• Using dsniff utility identify network administrator password while making telnet to switches or routers •	Requires that administrator will use telnet, ftp or other non secure protocols. However most of Cisco switches and routers, if not updated to latest versions can not run ssh and if yes will use ssh ver 1, that is still vulnerable to dsniff attacks
Trick the administrator to enter his username/password while he thinks that he connects to one of the hosts	• Identify IP address of routers, switches, OpenBSD Firewall, Web server • Perform arp poisoning on the router, so packets with destination IP of the network system will be sent to mac address of my server running ssh • Get the administrator password as soon he connects	Requires that administrator will not put attention to the message that server public key was changed. Most of the chances that it will work, but cautious administrator can start to suspect
Identify vulnerable hosts behind the internal Firewall	• Sniff for the traffic designated to subnet behind the Firewall and in this way identify the open ports on the Firewall and on the systems behind it 1. Scan for vulnerabilities on the open ports OR 2. If system downloads data	1. Requires that system behind the Firewall will be vulnerable. If all the systems are patched on time, might be not the case. 2. Download is not enough. Still need to find a way to execute the program

	from the servers before the firewall, use it to download Trojan to the system behind the Firewall	
Get access to the internal Firewall (OpebBSD with pf packet filtering)	• Exploit one of the OpenBSD vulnerabilities • To reduce risk of attack notification, can first spread some worm in the LAN that will exhaust all the logs and take care of the security people to fight the worm…	Risk to be recognized during the vulnerability scanning, because Firewall logs are usually watched closely

Connecting to "Secure Application Server"

This is the final target of the attack. According the design paper, I don't know which OS is used or which open ports the server has.
The Application server is located behind the internal Firewall along with syslog system and system administrator hosts. It is also located on different switch.
There is no information in the paper how exactly "Secure Application Server" gets proverbs from Production Application Server that is located in LAN area. If the method is FTP, it will make my task much easier. However I believe that SSH is used. The attack on the server will be performed from the "Main Server" on which I installed the backdoor and other tools.
To sniff on the switch, I will use dsniff option of arpredirect for all traffic aimed to Internal Firewall interface:
arpredirect *ip_address_of_internal_firewall*

and activate IP forwarding on our system, so the redirected traffic will eventually go to the Firewall:
fragrouter –B1

From sniffing, I identified (fingerprinting for OS was done with p0f application: p0f –s xxx.cap):

- syslog server (UDP port 514). Linux 2.4.2 . All Network equipment sending syslog messages to it
- Win2000 work station used for management connections – a lot of ssh connections to Network equipment and Production Application Server
- Probably Secure Application Server I am looking for – Linux 2.4.2, connects with ssh ver 3 to Production Application Server and WEB servers in DMZ.

(I must make some assumptions, because in the Marc design no details regarding OpenBSD firewall configuration, syslog or management station info)

The Windows workstation is the vulnerable system I was looking for, because it is also used for connecting to web on http with probably Internet Explorer.

Using “webspy” utility of dsniff, I will learn the web sites that are connected from Windows management station.
To take control over this machine, I will redirect the request for this site to my computer, will show some error message and in that time try to exploit by using the latest Explorer “HTML Help vulnerability” (MS04-023, CAN-2003-1041) and in parallel to download malicious ActiveX control. If internal web site is accessed the chance that security zone of MS explorer will be set to ‘Trusted Sites” that is usually allows free ActiveX uploads.
Redirection will be done with dsniff arp poisoning options arpredirect.
The HTML Help vulnerability - “vulnerability exists in the processing of a specially crafted showHelp URL. The vulnerability could allow malicious code to run in the Local Machine security zone in Internet Explorer, which could allow an attacker to take complete control of an affected system.”
Malicious ActiveX can be written according “Safe for Scripting” vulnerability. The explanation how to do it can be found on http://www.guninski.com/scrtlb.html or http://wwwatstake.com/research/advisories/2000/ouahack/index.html .
I will use this vulnerability to download and execute backdoor with Reverse WWW Shell. As soon I will have the backdoor opened, I will download BO2K like I did with my attack on the ”Main Server” and will use [Key Logging] -> [Log Keystrokes] BO2K option. This capability allows to store in the local file keys typed into each window. Now I need only wait pationtly till the administarator will connect to “Secure Application Server” and get his ssh password on the system.

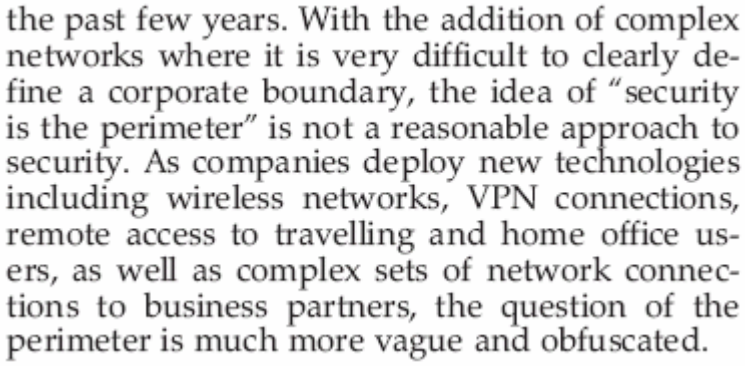
Assignment 4A - Future state of security technology

Network Security Management Architecture for Large Networks

Abstract

Following lately worms attacks, the large networks moving to segmentation/access control for “worm contentment, increased value of IDS/IPS and streamlined incident handling” [1]. ACLs on LAN routers, internal Firewalls and IPS systems are used for segmentation.

However such course brings new problem of security management. The classical model was highly protected Internet gateway with vast majority of security effort concentrated there. The new model suggests in large Networks hundreds of ACLs, Firewalls, IDS and IPS all over the Network. [3] summarize the problem statement: "


the past few years. With the addition of complex networks where it is very difficult to clearly define a corporate boundary, the idea of "security is the perimeter" is not a reasonable approach to security. As companies deploy new technologies including wireless networks, VPN connections, remote access to travelling and home office users, as well as complex sets of network connections to business partners, the question of the perimeter is much more vague and obfuscated.

"

This paper discusses concepts to simplify and improve Network Security manageability in large and complex from security point of view Networks.

The main goals of my proposed concept are:

- Reduce Total Cost of Ownership (TCO) for security management
- Allow fast event detection
- Allow fast and reliable emergency response
- Simplify security audits, communication problems troubleshooting and log analysis

Introduction

FCAPS model

ISO FCAPS IT extended framework suggests the following manageability scheme [2] :

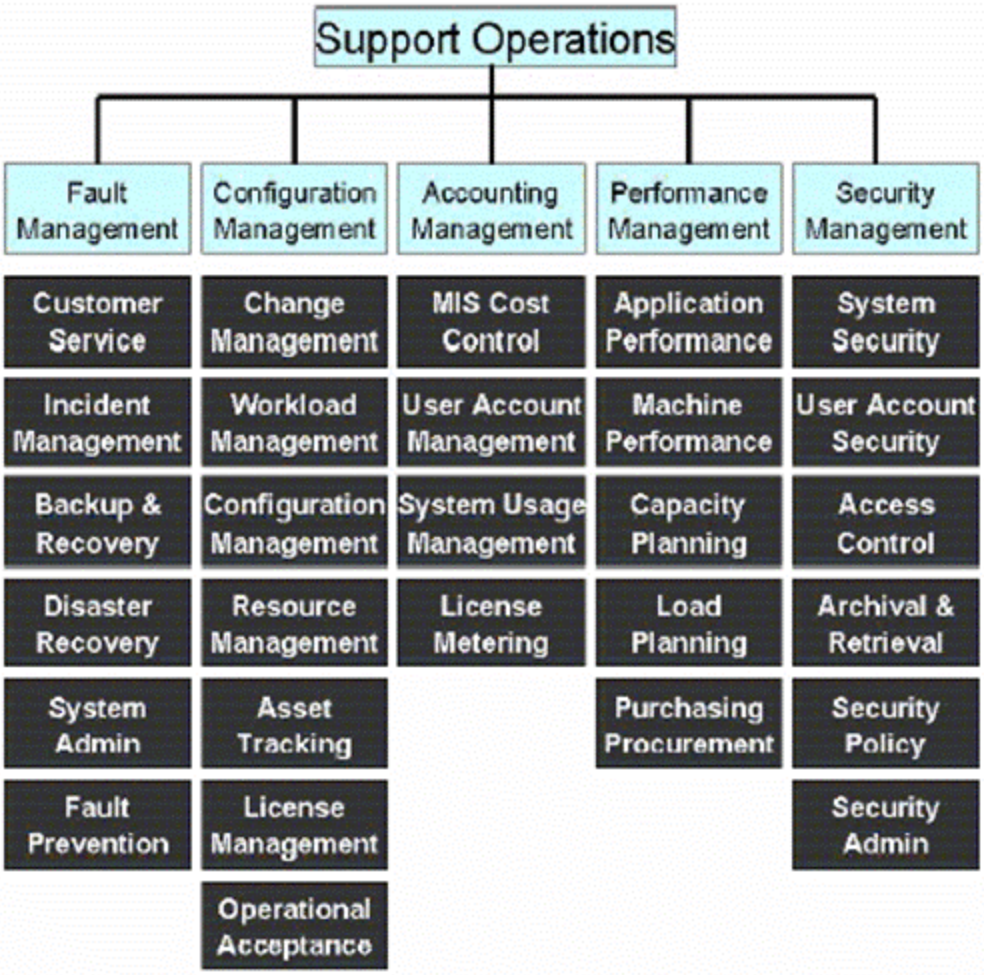


FIGURE 2 ISO FCAPS IT Extended Framework

The Security Management of FCAPS is however usually lacking the details needed to maintain efficiently Network Security.
Scot Wilson in his Security Management article [3], suggests “Extended FCAPS Model”:

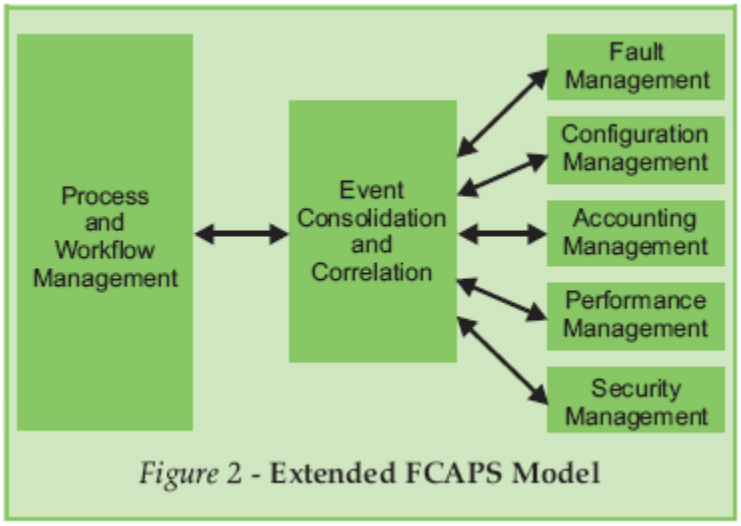


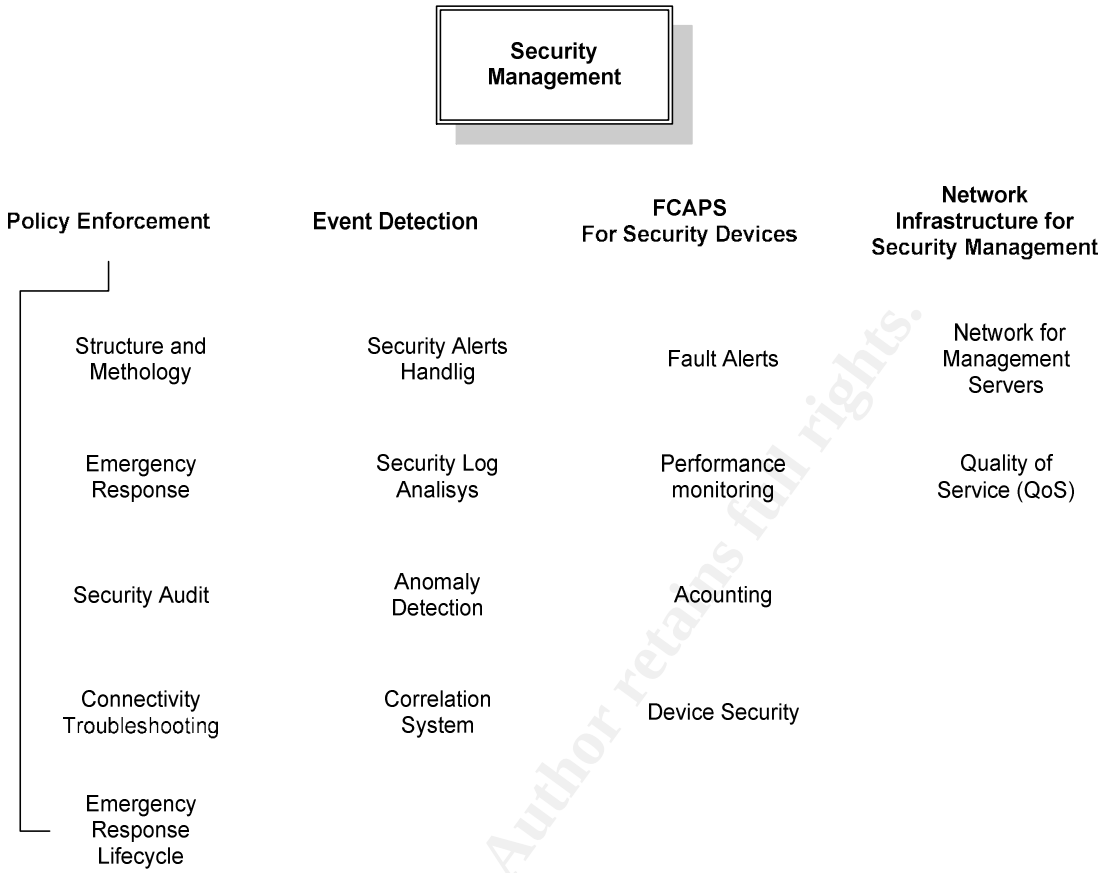
Figure 2 - Extended FCAPS Model

This model suggests additional correlation function between all the components and workflow management based on the correlated data. For example during worm attack we will see increased network activity, increased CPU values on servers/routers, etc…

In my work, I would like to propose more detailed Framework for Network Security Management that will try to cover other aspects of the management like policy enforcement and more detailed view on event detection and FCAPS.

Security Management Framework

I would like to propose the following framework:



- Policy Enforcement will define how to add security policies/rules to enforcement points like routers, firewalls, IPS and IDS during normal and crisis situations. It will help as well to perform security audits and connectivity troubleshooting
- Event Detection will define how to identify efficiently attacks in every point of the Network
- FCAPS for security devices will only follow the existing well defined model for management of any IT equipment. We will concentrate more on the FCAPS for Security equipment – Firewalls, Routers with acls, Proxies, IPS and IDS
- Network infrastructure for security Management should ensure that our management servers are located on highly available and secured Networks
-

Definitions

I will use definitions by Mitchell Rowton [4]:

" **Enclaves-** For the purpose of this policy an enclave is defined as a system which requires an independent security classification from other systems. Example enclaves could include: DMZ(s), server networks, host networks, or extranet systems"

"**Defense in Depth (DiD):** Firewalls cannot only be placed at the perimeter of the **Company** network; firewalls must also be strategically placed among enclaves in the **Company** network

in which management decides that the benefits of this protection overcome the resources involved in installing and managing the firewall"

As well I will use term of "Enclave Enforcement Point" or EEP to indicate host that enforce security policy like Firewalls, Routers with ACLs, Proxies, …

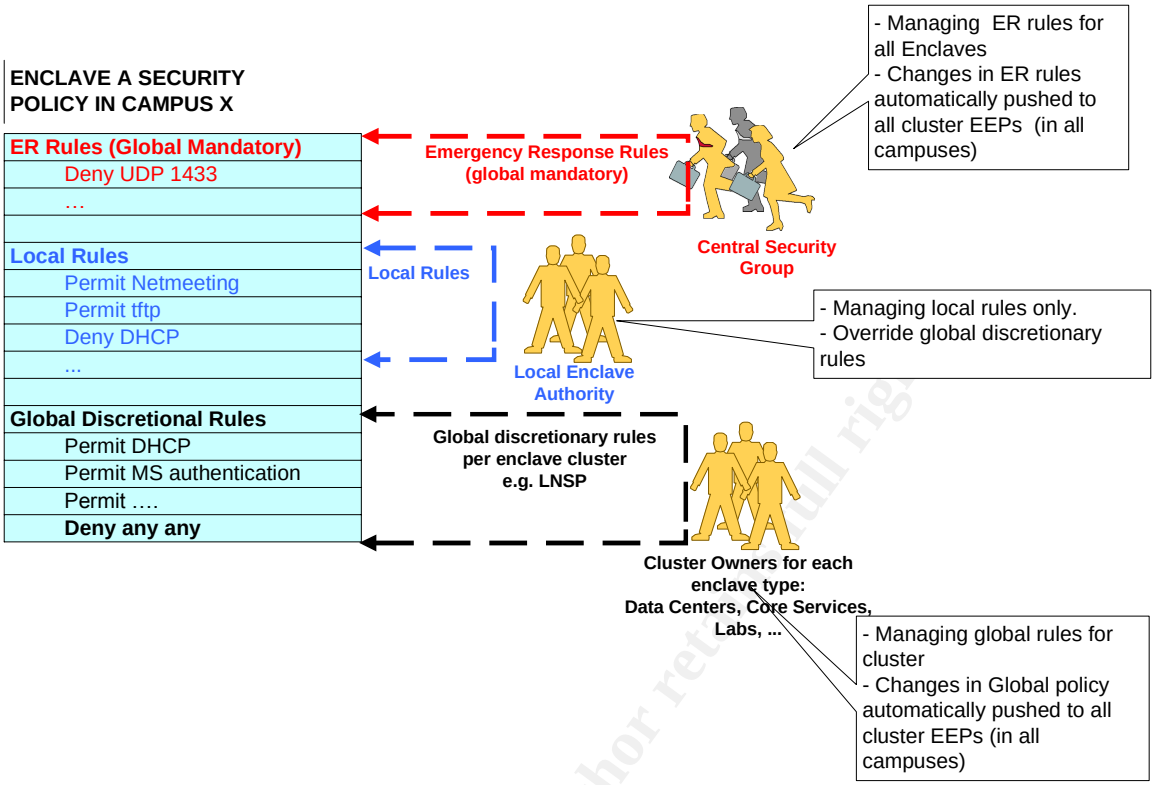
Policy enforcement

Structure and sustaining methodology

In large corporate networks spreaded over different countries and continents, you can not count on one central group to manage all the internal security (the perimeter security will be managed usually by single central group). When I speak regarding internal security I mean ACLs on the LAN routers, internal Firewalls and local Intrusion Protection Systems (IPS) that as stated in the abstract are used more and more (e.g. [1]).
On day to day basis those internal policies can be changed according introduction of new systems, new applications, system upgrades, etc… It is almost impossible for one remote group to manage all the changes. However during crisis situation, like worm spread, we would like central security group to define the ACLs and Firewalls rules to be implemented to stop the worm.
Additional requirement to reduce the management overhead is to have same policies for same Network segments types (or how they are usually called network enclaves). For example packet filtering rules on Data Center borders will be basically same for all Data Centers in corporate and rules to protect development Labs might be quite similar for every Lab (e.g. accept inbound ssh and ftp).

The following security policy architecture is to support the above requirement for every enclave:

1. Fast emergency Response performed by central group
2. Easy day to day sustaining of the enclave policy changes by local support
3. Easy implementation of new enclave



The concept is that security rules will be divided into three logical pieces:

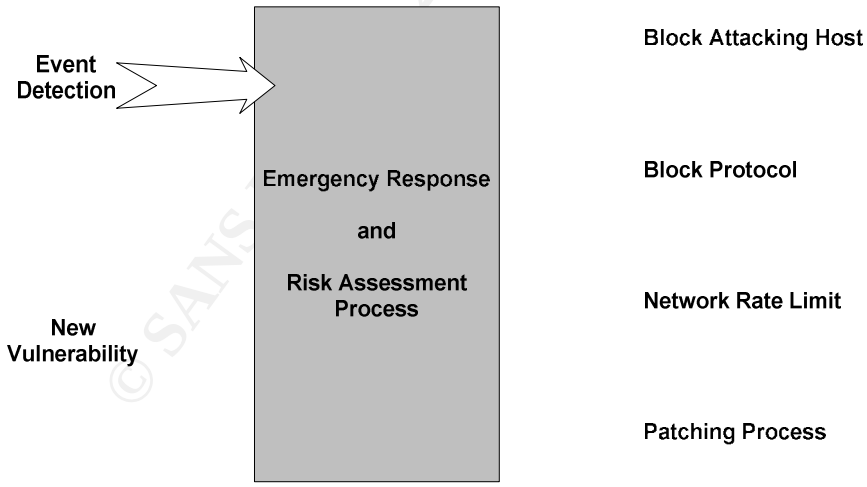
1. **Global Discretional Rules:**
   a. Defined by enclave owners and applied at the **bottom** of the rule set. There should be a tool to allow push/pull of the Policy changes to all relevant enclave enforcement points (Router ACLs and Firewalls). (For example for ACLs, we can use standard remark starting this part of the rules. The automated tool can pull the relevant ACL, replace the rules below the remark and push the new one back)
   b. To make it successive the tool must have a Database with all local servers like local DNS, local mail, local Domain Controllers and replace the relevant object with correct values for each site
   For example the following Global rule:
   permit tcp any #Site#&&#Domain_Controller# range 135 139 log
   with "London" as parameter for site will retrieve the relevant information from database and create the correct rule (with remark) for London site:
   remark **** London Domain Controller
   permit tcp any 10.1.1.99 0.0.0.0 range 135 139 log
   c. Those rules can be overwritten by local people. For example if Global Discretional rule for Lab enclaves allows DHCP requests from the lab, in one specific lab the local owner can deny DHCP
   d. Those rules ensure standardization between enclaves of the same type and reduce the workload on local people to configure enclave

policies. Basically Global Discretional Rules should cover all the enclave requirement, thus leaving to local people dealing with very small number of discrepancies between different sites

2. **Local Rules**
    a. Managed by local IT operation. Will include all site specific rules that are in addition to Global
3. **Emergency Response (ER) Rules**
    a. This part is managed by Central Security Group. The main purpose is to be able to push centrally rules that will help to stop worm propagations or host identified as attacking by IDS systems. The tool should allow to add/change rules in this section without changing the local and global discretional rules
    b. Example can be SQL Slammer worm, where urgent "deny udp any any 1433" should be applied across all the enforcement points "as soon as possible"
    c. It is very important to have "life cycle" process for ER rules, otherwise this section will become full with unneeded rules and might create unnecessary communication problems

Emergency Response

I would divide emergency response to four main categories: blocking attacking host(s), blocking protocol/vulnerability, applying rate limit/QoS and patching process.
The emergency response would normally initiated by main two events – event detection and vulnerability alert (e.g. new bugtraq post)



I will not suggest specific Risk Assessment process. Every company should create such process with appropriate people from Security, Business and IT operation organizations. There is plenty of material in this area e.g. [5] or [6].

I will concentrate on the tools that should exist to perform efficient and fast mitigation of the identified risk or attack during crisis situations.

As with any emergency response action, “life cycle” process must be established. Blocked hosts and protocols should be recorded and process for removing the blocks automatically and/or manually must be established.

1. Blocking attacking host(s)
    a. To block externally located attacking host specific rule should be applied to appropriate security policy. Usually it will be ACL on the router facing the attacking host. The methodology suggested in previous section should allow fast addition of blocking rule to ER rules section and pushing it to the enforcement points
    b. To block internally located host, in addition to ACL, we can disable (or rate limit) Switch port the attacking host is connected. To perform this task Database with IP to MAC to Switch port mapping must exist. There are existing tools to make this mapping like CiscoWorks for Cisco switches. It can be also accomplished by getting arp information from Routers (show ip arp), mac information from switches (show cam dynamic) and correlating the two lists.
2. Block protocol
    a. The methodology suggested in previous section should allow fast addition of blocking rule to ER rules section and pushing it to the enforcement points. Usually will be used during worm attack. For example to mitigate SQL slammer propagation udp and tcp 1433 should be blocked where possible. For example on client enclave it can be done quite safely, because critical to organization SQL traffic will be usually between servers.
3. Rate limit
    a. In my opinion underestimated tool to mitigate worm spreading as soon started. Process to reduce rate limit on non server’s enclaves should exists and activated during crisis situations
4. Patching process
    a. No magic here. Plenty of material on how to establish this process available. Three good references are Felicia M. Nicastro, Security Patch Management paper [7], [8] and US General Accounting Office (GAO) statement on effective patch management [9]. The process should cover OS and Application patches as well as Antivirus updates and is crucial for Corp systems durability.

Security Audits

On-going audits needed for patch/antivirus versions and security policies on enclave borders.

1. Patch versions
    a. It is important to ensure that all your hosts and especially critical servers are patched according the last Risk Assessment decision.

For specific vulnerabilities dedicated scanners exist and can be used. However, in large networks we would like to get report on antivirus, main OS and Applications (like Internet Explorer) versions. There are existing products like GFI LANguard Network Security Scanner (http://www.gfi.com/lannetscan/?adclickid=1416933) or Shavlik HFNetChkPro (www.shavlick.com)

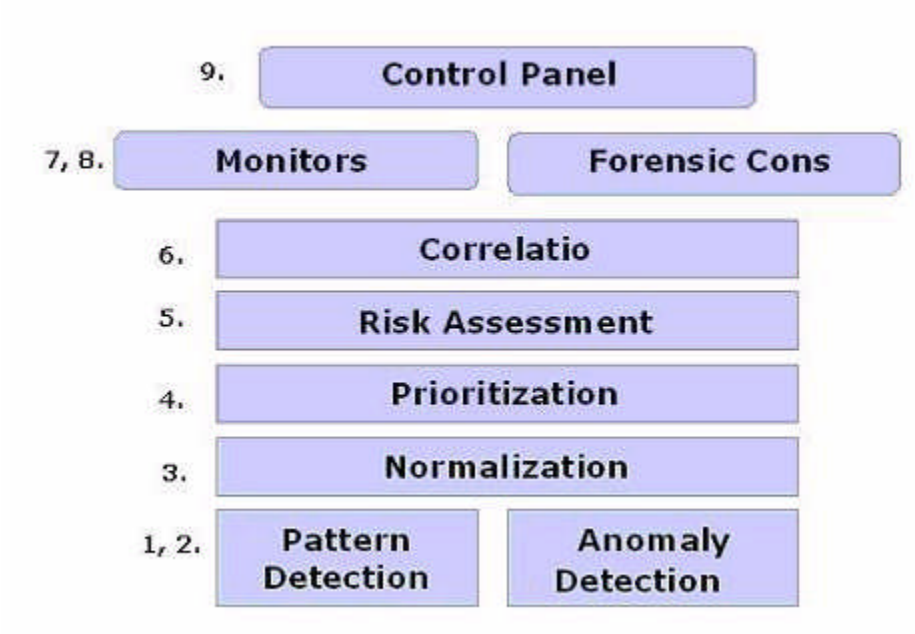
2. Security Policy monitoring
    a. It is impractical to perform real penetration scanning in large corporation for internal security on day to day basis. I would suggest providing an easy tool for Security audits based on queries of security policy on enforcement points. Example can be “list all IT Core Services Enclaves with permitted inbound TCP 135 port” or “list all enclaves without deny udp 1433 rule”. This tool should be based on Security Policy management tool suggested in previous paragraph

Connectivity Troubleshooting

Internal segmentation and introduction of internal enclaves introduce new challenge for network operations. The old and perfect troubleshooting tools like “ping” and “traceroute” might not work because of security policies. Even they will work it will not say anything regarding applications connectivity. In such environment application and network layer troubleshooting tools should be developed. One of the tools might be the same tool proposed for Security audits. More advance method like wide usage of sniffers, log analysis tools for blocked packets on enforcement points and training on “beyond layer 3” protocols to Network personnel might be required.

Event Detection

Obviously Event Detection is essential part of Security. However detection is becoming more and more difficult given the complexity of Security infrastructure. Huge amount of information is flowing to us from IDSs, Firewall logs, Routers logs, system logs, network activity monitoring, etc …from hundreds sources. Attack identification in such case can be like looking “a needle in a haystack”. The most extensive work on the Event Detection management was done by OSSIM (Open Source Security Information Management) group [10]. Their work is not only excellent theoretical reference, but also open source tool that can be used.
The functionality provided by OSSIM tool is:



from [10]

I will give short summary of what are Event Detection components and how I see the establishment of such system in large corporate

Security Alerts handling

Security alerts are mainly coming from IDS and IPS systems. Most of the Firewalls in addition to logging can also produce alerts on what they assume as attack. The problem with all those alerts is extremely high rate of false positives. In highly segmented network with tens IDS systems, the rate of alerts and false positives can become unmanageable.
I would suggest to use “Mid Level Manager” (MLM) per campus (or other logical division). The purpose of this system is to reduce number of alerts reaching the Security main management system. OSSIM tool can be used for this purpose. Other option that MLM will make some statistical analysis like in anomaly detection and will forward to central management only abnormal data. Of coarse such approach can create false negatives (missing real event). This is a good reason to use OSSIM approach for prioritizing events before final correlation. Event from Internet gateway should be treated differently than event generated by IDS on client enclave. Port scanning alert should be treated differently than alert with Nimda worm signature.

Security Log Analysis

In large networks manual log analysis is practically impossible. The logs are generated by Routers, Firewalls, Servers, IDS and IPS systems. In large networks it will come to hundreds of logs. Each system usually have it’s own unique log format even if both systems write to syslog for example.

The only way I see it, is to create automated reports based on log files and to examine only “top 10” or abnormal values. After identifying anomaly, drill down to actual data can be done.
There are quite a lot existing log analisys tools like Checkpoint Reporter for Checkpoint logs and WebTrends. Summary of different tools scan be found on http://is-it-true.org/fw/fwtips12.shtml . Specific attention should be done on logreport.org (http://www.logreport.org/) and their Lire project [11], the open source log analyzer for very big number of different logs.
As with security alerts, I would suggest to have “Mid Level Manager” (MLM) and automatically forward to central security group only “top 10” and abnormal summaries from each MLM. The definition for “abnormal” should be defined as well according the priority of specific log.

Anomaly Detection

Anomaly detection is most important on Network level (e.g. extremely high number of MS-RPC sessions), system level (e.g. high CPU) and access level (e.g. high number of system access on management port).
Anomaly is always done by recording enough data to create a baseline and then compare each sampling to the base line.
There are a lot of commercial tools for Network anomaly detection. System data anomalies can be done with free tools like RRD. As discussed in previous section on log analysis, anomalies can be effectively found through logs as well.
Bottom line – extremely important tool for large corporate, that must be taken into your Security Management toolbox

Correlation

Automatic correlation is probably most difficult part of the Event Detection. The correlation process should take the inputs from Security Alerts, Log analysis and anomaly detection and pinpoint on the attack. For example worm detection might be not complicated task: Network Anomaly detection will point on abnormal activity on some specific port, Firewall logs will see a lot of dropped packets on the same port and “port scanning” security alerts will be sent. But, for example, correlation of inputs that will suggest slow network probing by attacker is not simple. You should probably see couple of extra log lines on different logs, but to conclude that “from this source IP address large number of host was probed in last 24 hours” is not a simple task.
OSSIM [10] suggest high level correlation between Network Anomaly detection (Spade) and IDS (Snort). Hopefully more tools will become available.
In any case correlation should be part of the Security Management framework because it can identify attacks that each single log of different equipment will not provide enough data

FCAPS for security devices

Not much I can add to extensive information on the model (e.g. [2]).
I will shortly summarize the most important aspects related to Security Devices

Fault Management

To get Fault alerts from all security equipment is extremely important. It will include Firewalls, IDS, syslog servers, Network management servers, etc… The alerts should be treated in “Critical” priority. The basic alerts are “system down”, “high CPU”, “disk full”, “process not running”, etc…
One must ensure that all security related equipment are monitored and sending Alerts

Performance Monitoring

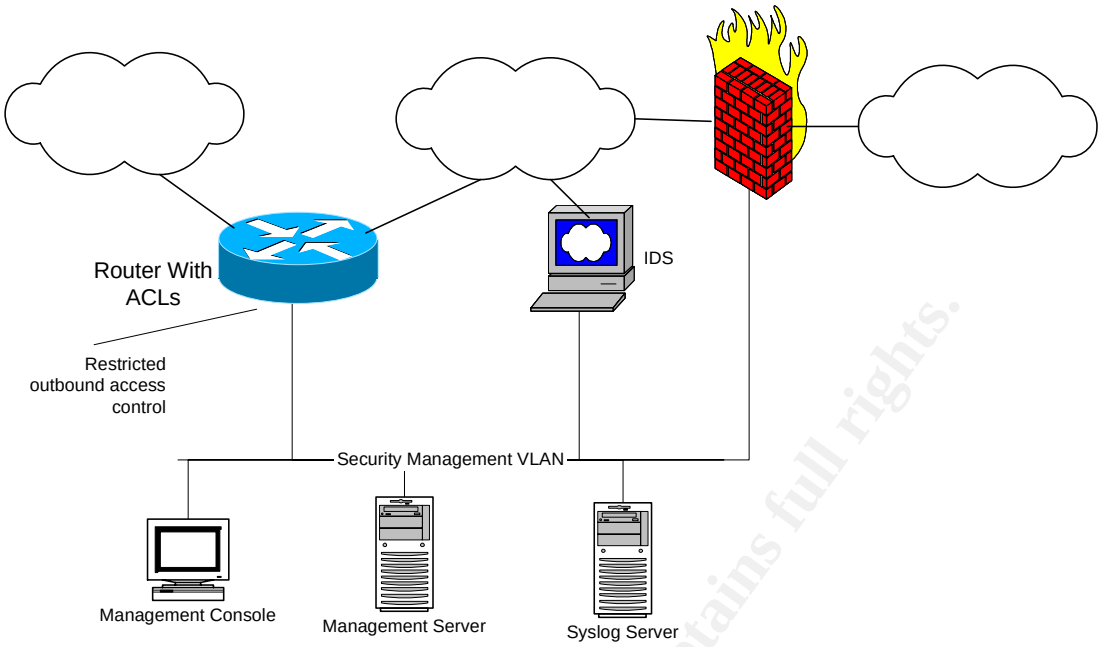
The main purpose of performance monitoring is for trend analysis. If you see constant increase in Firewall CPU, you can estimate when it will reach unacceptable levels. The same is true regarding network utilization, disk space on syslog server, etc…
To pick the most important ones to monitor, I would suggest Network traffic through FW or Routers interfaces, CPU, and number of logged entries. On Firewalls number of dropped packets as well.
However beside trend analysis this data can be used as Event Detection tool as well. Sudden increase in Network traffic rate or logged entries rate can indicate attack

Equipment Security

To serve as a model for security, we must ensure that all our equipment is: patched, implement strong password, change passwords policy and doesn’t have unneeded open ports. This should include all the components like enforcement points, management servers, IDS, etc…

Network Infrastructure for Security Management

The last aspect of suggested framework is Security Management network. I strongly believe that all Security devices should be managed from secured network with access control. In addition we can design this network to be highly available and more durable during worm attacks or Network failures. Added value can be in configuring QoS for traffic to/from the management subnet. Guaranteed bandwidth will allow communication to the subnet during Network overload or worm situations.



For paranoids the access to the Management Network can be restricted per user. User authentication can be performed by most of the current Firewalls. Additional feature to be considered is access from home to management network during Network issues or DoS attack. The easiest way is to have phone connection to some RAS service on the network. This line can be disconnected on regular basis and connected by people on-site during crisis. Other option can be to have PPTP connection (e.g. DSL) from system that can be VPN server (e.g. Checkpoint S-Box)

References

[1] Deterding, Brent. “Segmenting Networks: ACLs”. 2004 , SANS Webcast

[2] Walker, Bill. Jun 2000 URL: http://www.sun.com/blueprints/0600/prodeng.pdf

[3] Wilson, Scott. “Security Management”. March 2003. URL: http://www.ins.com/downloads/publications/Security_Management.pdf

[4] Rowton, Mitchell. “Enclave Boundary Defense Policy”. 2003. URL: http://www.attackprevention.com/ap/library/enclaveboundarydefense.htm

[5] FFIEC InfoBase. “Information Security Risk Assessment”. 2002. URL: http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/02_info_security_%20risk_asst.htm

[6] U.S. General Accounting Office. “Information Security Risk Assessment”. Aug 1999 URL: http://www.gao.gov/special.pubs/ai99139.pdf

[7] M. Nicastro, Felicia. “Security Patch Management”. March 2003. URL: http://www.ins.com/downloads/whitepapers/ins_white_paper_security_patch_mgmt_0303.pdf

[8] “Security Patch Management In An Enterprise Environment”. 5 January, 2004. URL: http://www.itsecurity.com/papers/unisys1.htm

[9] U.S. General Accounting Office. “Effective Patch Management”. 10 Sep 2003. URL: http://www.gao.gov/new.items/d031138t.pdf

[10] Open Source Security Information Management Organization. URL: http://www.ossim.net/home.php

[11] Stichting LogReport Foundation. URL: http://www.logreport.org/lire/