

CheckPoint Software Technologies LTD.ä

OPSEC application Usage with Check Point FireWall-1 and VPN-1

Event: Partner Exchange Conference

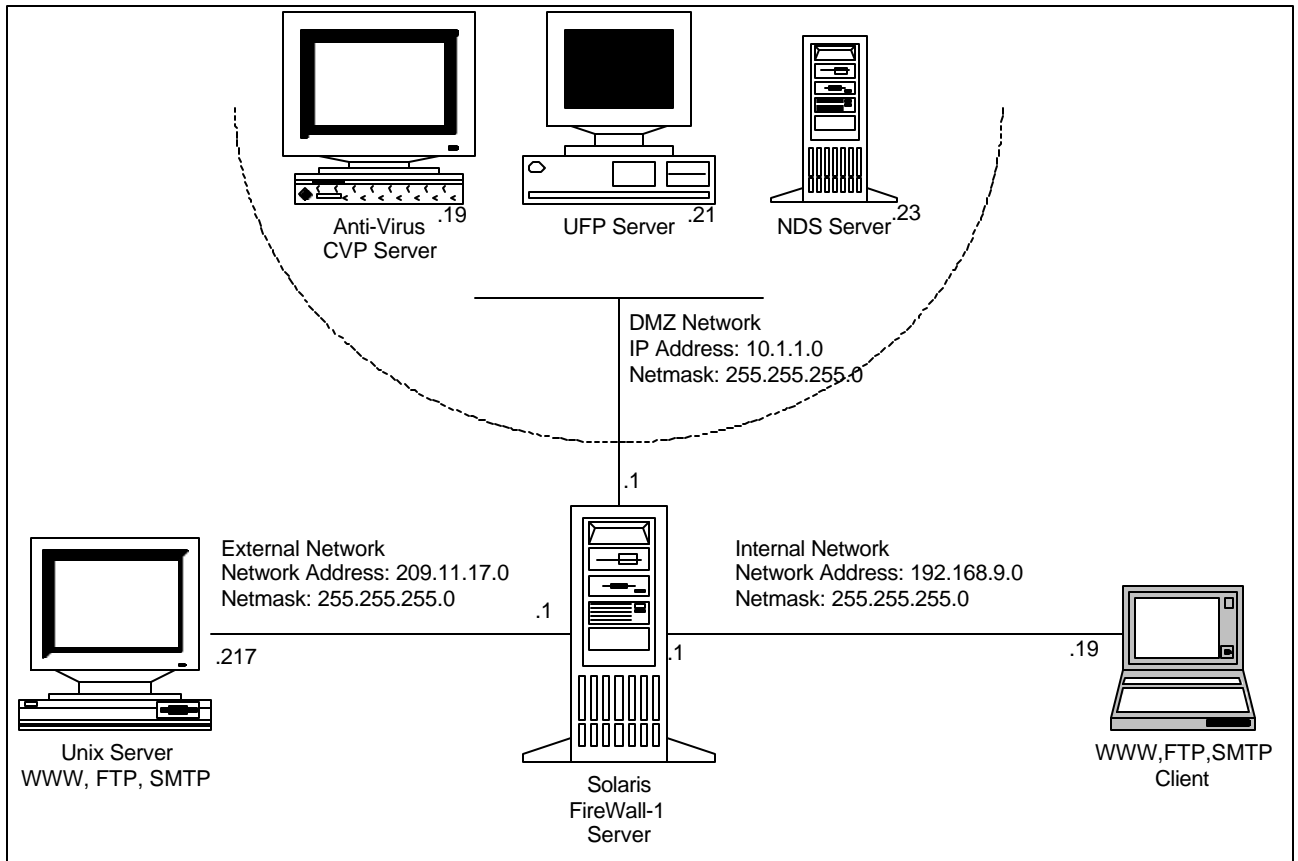
Date: October 20, 1999

Revision 1.0

Author: Todd Ignasiak

Credits: Upesh Patel

Diagram of Customer Scenario:



Goal of Demo:

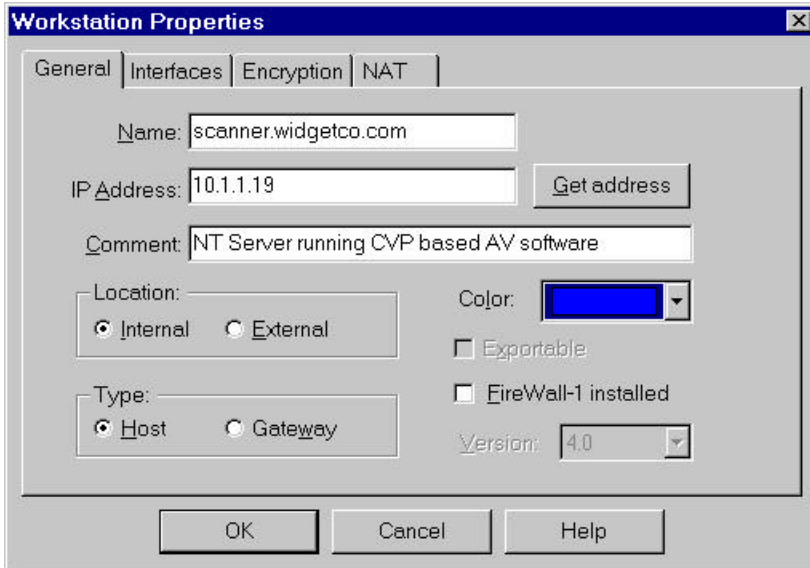
Demonstrate the tight integration of OPSEC certified applications, using both OPSEC API's and open standard interfaces.

Equipment Needed:

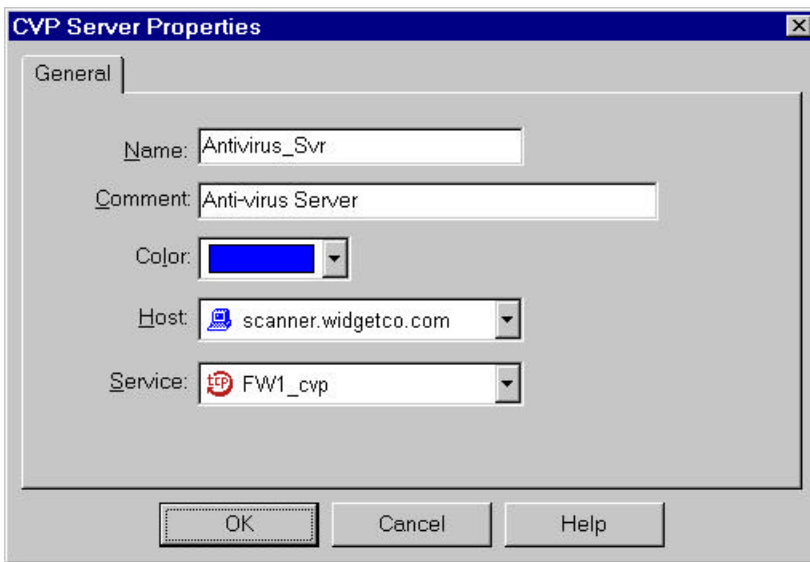
FireWall-1 version 4.0 or newer (Solaris version used in demo)
OPSEC Certified Virus Scanning Software (NT based product used in demo)
OPSEC Certified URL Filtering product (NT based product used in demo)
Novell NDS Server on x86 hardware
Windows 98 Client on laptop, Novell client software for NDS management
Unix Server – Linux based server on x86 hardware

UFP/CVP Installation and Configuration:

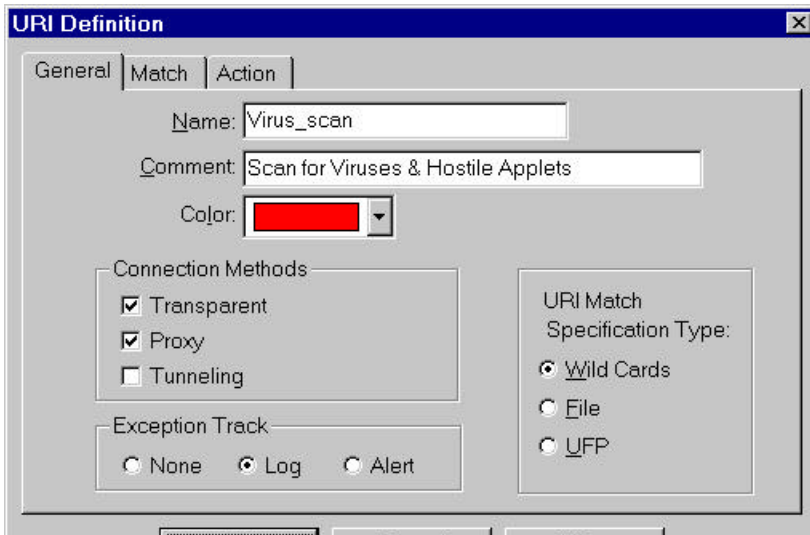
1. Install UFP and CVP server software. Windows based installshield installation.
2. Configure FireWall-1 objects and resources
 - a. Define Workstation objects for servers (Manage->Network Objects)



b. Define CVP Server Objects (Manage->Servers)



c. Define CVP Resource Objects (Manage->Resources)

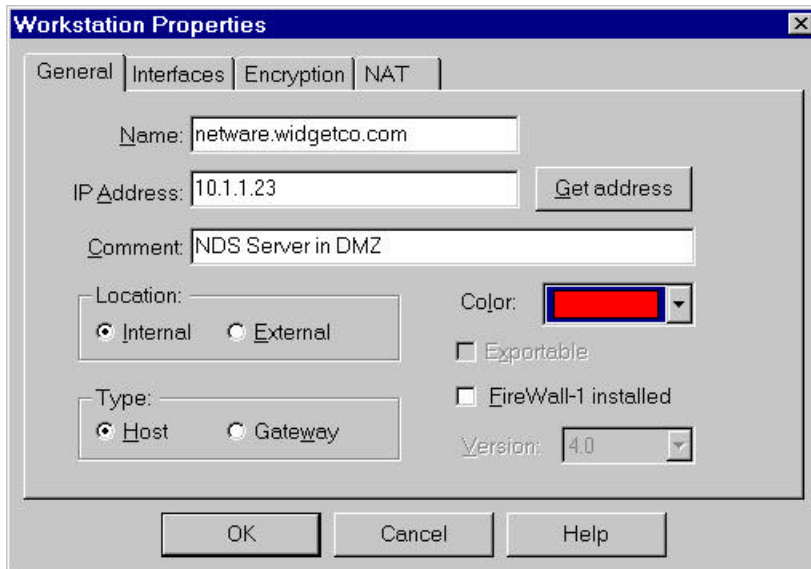


- d. Configure the firewall to enable the resources. Right click in the Service field, and select “Add with Resource”.

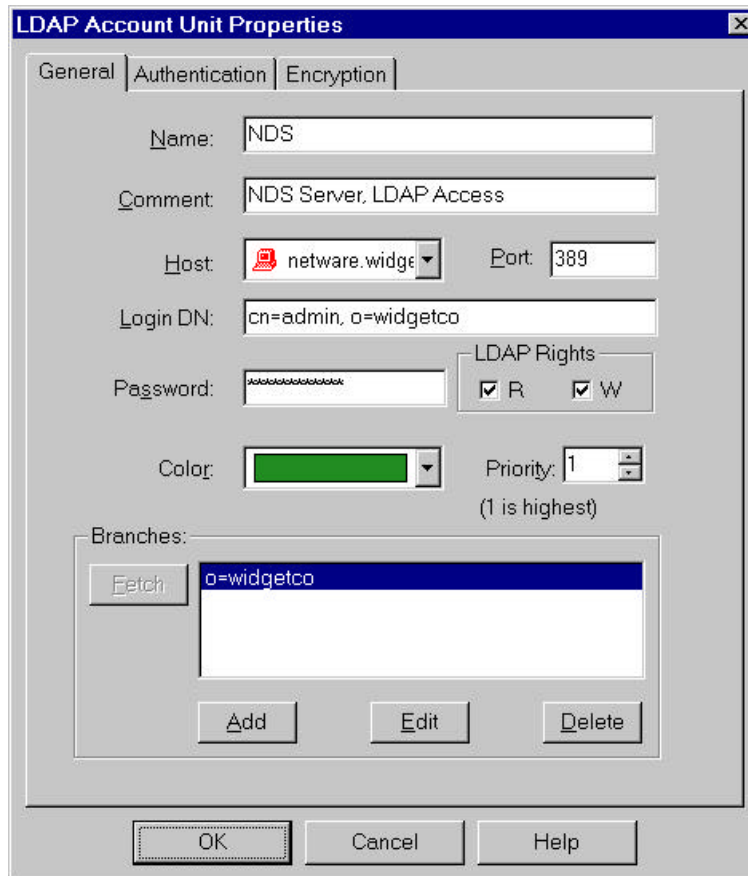
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Exec_mgmt	Any	http	accept	Short	Firewall	Any	Allow unrestricted http access for exec's
2	Corporate_Net	Any	http->URL_Filter	reject	Long	Firewall	Any	Reject access to WWW sites containing Sports/News.
3	Corporate_Net	Any	http->Virus_scan ftp->FTP_Filter smtp->Scan_Mail	accept	Long	Firewall	Any	Virus Scan ftp, http, and smtp
4	Supplier_Net	Corporate_Net	ftp TNS270 H323	Encrypt	Long	Firewall	Any	Allow Supplier access to selected protocols via VPN tunnel.
5	Any	DMZ	http	accept	Long	Firewall	Any	Allow external access to WWW server in DMZ
6	NDS_Users@Corporate_Net	Any	telnet	User Auth	Account	Firewall	Any	Allow outbound telnet if user authenticates
7	Any	Any	Any	drop	Alert	Gateways	Any	Disallow all other traffic and send an alert if encountered.

NDS User Authentication Configuration:

1. Define Workstation Object for NDS Server (Manage->Network Objects)



2. Define an LDAP Account Unit for the NDS Users



3. Define External User Group (Manage->Users):

General

Name: Color:

Comment:

Acct Unit:

Group's Scope

All Account-Unit's Users

Only SubTree ([optional prefix] , branch):

Only Group in branch (DN prefix):

OK Cancel Help

4. Define user authentication rule in firewall:

AccessControl - VPN-1 & FireWall-1 Security Policy

File Edit View Manage Policy Window Help

Security Policy | Address Translation

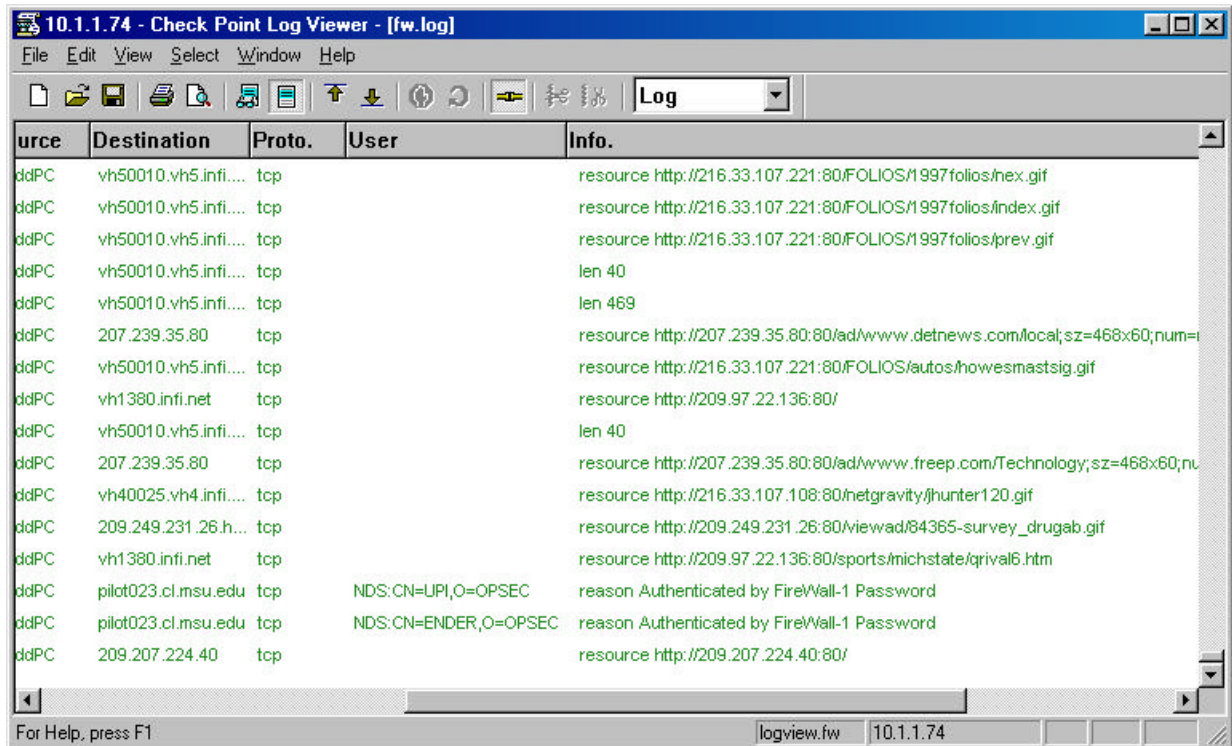
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Exec_mgmt	Any	Ntp	accept	Short	Firewall	Any	Allow unrestricted http access for exec's
2	Corporate_Net	Any	http->URL_Filter	reject	Long	Firewall	Any	Reject access to WWW sites containing Sports/News.
3	Corporate_Net	Any	http->Virus_scan ftp->FTP_Filter smtp->Scan_Mail	accept	Long	Firewall	Any	Virus Scan ftp, http, and smtp
4	Supplier_Net	Corporate_Net	ftp TCP3270 H323	Encrypt	Long	Firewall	Any	Allow Supplier access to selected protocols via VPN tunnel.
5	Any	DMZ	http	accept	Long	Firewall	Any	Allow external access to WWW server in DMZ.
6	NDS_Users@Corporate_Net	Any	telnet	User Auth	Account	Firewall	Any	Allow outbound telnet if user authenticates.
7	Any	Any	Any	drop	Alert	Gateways	Any	Disallow all other traffic and send an alert if encountered.

For Help, press F1

Local Read/Write NUM

Confirming the configuration:

Logviewer – Once the resources are enabled, additional logging information will be available in the log viewer. For example, in the image below the URL's for each HTTP connection are shown. If a virus is found this will also be shown in the log. Also, for authenticated connections the user name is shown. In this example, the user was authenticated via LDAP through NDS and the user's Distinguished Name (DN) is shown.



Source	Destination	Proto.	User	Info.
ddPC	vh50010.vh5.infi....	tcp		resource http://216.33.107.221:80/FOLIOS/1997folios/nex.gif
ddPC	vh50010.vh5.infi....	tcp		resource http://216.33.107.221:80/FOLIOS/1997folios/index.gif
ddPC	vh50010.vh5.infi....	tcp		resource http://216.33.107.221:80/FOLIOS/1997folios/prev.gif
ddPC	vh50010.vh5.infi....	tcp		len 40
ddPC	vh50010.vh5.infi....	tcp		len 469
ddPC	207.239.35.80	tcp		resource http://207.239.35.80:80/ad/www.detnews.com/local;sz=468x60;num=
ddPC	vh50010.vh5.infi....	tcp		resource http://216.33.107.221:80/FOLIOS/autos/howesmastsig.gif
ddPC	vh1380.infi.net	tcp		resource http://209.97.22.136:80/
ddPC	vh50010.vh5.infi....	tcp		len 40
ddPC	207.239.35.80	tcp		resource http://207.239.35.80:80/ad/www.freep.com/Technology;sz=468x60;nu
ddPC	vh40025.vh4.infi....	tcp		resource http://216.33.107.108:80/netgravity/jhunter120.gif
ddPC	209.249.231.26.h...	tcp		resource http://209.249.231.26:80/viewad/84365-survey_drugab.gif
ddPC	vh1380.infi.net	tcp		resource http://209.97.22.136:80/sports/michstate/qival6.htm
ddPC	pilot023.ci.msu.edu	tcp	NDS:CN=UPI,O=OPSEC	reason Authenticated by FireWall-1 Password
ddPC	pilot023.ci.msu.edu	tcp	NDS:CN=ENDER,O=OPSEC	reason Authenticated by FireWall-1 Password
ddPC	209.207.224.40	tcp		resource http://209.207.224.40:80/

CVP connections can be confirmed by showing the open connections on the firewall, while making CVP requests, “netstat -an | grep 18181”.

The firewall connection table can also be used to determine if the security server is processing connections. For example, to verify that HTTP sessions are being processed, use “fw tab | grep 80”.

Networking sniffing tools, such as ‘snoop’ on a Solaris machine can also be used to confirm that CVP or LDAP requests are being made by the firewall. By default, CVP uses TCP port 18181, and LDAP uses TCP port 389. (e.g. “snoop -d qfe0 port 18181” where qfe0 is the name of the ethernet interface the CVP connections are being sent on)

When configuring LDAP authentication, please confirm the appropriate settings with the administrators of the directory server. Errors in the administrator's DN (e.g. “cn=admin, o=checkpoint”) or branch definition (e.g. “o=checkpoint”) will cause problems.