Check Point Software Technologies LTD.™

How to Configure the Firewall to Block a Port Scan using SAMP and Check Point Real Secure
Goal of the Demo:
- Demonstrate the re-configuration of the FireWall based on the detection of an attack from an external device.
- Demonstrate the Suspicious Activity Monitoring Protocol (SAMP) capability of the Firewall. Show the "sam_blocked_ips" table using "fw tab" command to verify the connections are being blocked.
- Demonstrate the ability of RealSecure to send real-time alerts to Administrators via SAMP if unauthorized traffic is being sent to FireWall and being dropped.

Network Diagram:

Necessary Equipment:
- Firewall-1 version 3.0B(3064) or greater (Unix or NT)
- UNIX or NT System for the Firewall.
- Windows 95/98 Client workstation as the Port Scanner station
- Port Scanner Software. (Netlab is available @ http://www.mato.demon.nl/frw/finger.htm )
- NT 4.0 Service Pack 3.0 for the RealSecure Machine
- NT 4.0 Service Pack 4.0 for web server test
The network is structured so that an external device, essentially on the Internet will launch the malicious attack against the VPN-1 Remotelink in our case a port scan. The RealSecure Engine will recognize the attack and respond in Real-Time by reconfiguring the Firewall. All networks are 192.32.X.X with the exception being the Internal Network, which is being hidden behind the FireWall.

Setup:
The FireWall has been configured with an ‘Open’ Security Policy. It will accept all traffic coming from and going to Any address using Any service. Netbios traffic has been filtered so it will be dropped and does not make any Log entries.

The client software used to attack the Firewall was a product called NetLab. Similar products are available to download from the Internet.
The port scanning product in NetLab was setup to launch a Port Scan directed towards 192.32.32.3 (outside interface of the FireWall).
Before configuring the RealSecure engine shared secret keys must be placed on both the FireWall and RealSecure Engine.

Configure OPSEC putkey from firewall to the RealSecure Engine and Back:

**On FireWall:**
$FWDIR/bin/fw putkey -opsec 192.32.32.10

**On RealSecure Engine:**
C:\Program Files\Check Point\RealSecure\opsec_putkey.exe 192.32.32.3

**NOTE:** The Check Point RealSecure Engine and Console can be configured on different servers. For this demo the Engine and Console are on the same system.

The RealSecure Engine and Console should then be configured. The Main Console screen from RealSecure is below:

First you must start by monitoring an engine. Click on **Engine -> Monitor Engine** in the GUI to connect the console to an available engine. Then click on the engine that you are monitoring and goto the **Properties** Section.
There are 10 Pre Defined policies, which cannot be edited. In order to have a customized policy you must create a new one. Click on the most restrictive policy “Maximum Coverage” then click on “Derive New Policy”. We gave ours the name Partner Event.

In order for the RealSecure engine to communicate with the Firewall after the putkey authentication is done the Engine must be told where the Firewall is and what to do if an attack is detected.
Under the Actions Tab of the Engine Properties double click on “Firewall-1”. This is where we set what actions RealSecure should take to the malicious connection. This is also where the FireWall Gateway to be monitored is specified. You can place the resolvable name or IP address of a Firewall Module or Management Server if you want the RS engine to reconfigure all the Firewall Modules of a given management server.

OPSEC authentication is also set here for the previously defined putkeys (page 5).
We will configure the RealSecure Engine to take action on any incidence of a Port Scan. RealSecure was configured to log the attack, kill the connection and reconfigure the Firewall to no longer accept any traffic from the malicious device. You can also have the attack recorded in a file for later review.
Once the Policy has been created and modified to monitor the network for the desired malicious activity, it must be applied to the RealSecure Engine. Click on “Apply To Engine”
Once the Policy is installed on the RealSecure Engine, and the attack is launched, the RealSecure engine detects it, kills the connection and reconfigures the FireWall by creating entries in the State Tables to block the connections from the source.

The Engine window shows the Policy that is running and its status. The window on the left shows the IP address an attack was detected from and what type of attack it was. By opening the High Priority event in the right window, all summary details about the attack are provided, including the source and destination addresses and what actions were taken by RealSecure to protect the network.
Entries in the Check Point log file show the attempted scan as it began then the quick action of the RealSecure engine once detected blocking the future connections as they occurred. Note that the rule number is *sam* indicating that this is a SAMP created rule. In the information section of the log entry you can get more detailed data about the SAMP rule and its duration.
If you need to delete the same rules on the Firewall Module or Management Server you can use the `fw sam` command to manipulate the SAMP rules. In version v4.1 of VPN-1/Firewall-1 this action is build into the log GUI.
Troubleshooting Guide:

The Log Viewer entry for the malicious session shows the details associated with the malicious session. It shows the address of the closed session and the time of expiration for its connections through the FireWall.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Info.</th>
</tr>
</thead>
</table>
| 192.32.32.10 | remotelink | started sending log to localhost
| 192.32.42.11 | remotelink | started sending log to localhost
| 192.32.32.10 | remotelink | installed Open
| 192.32.42.11 | remotelink | len 40
| 192.32.32.11 | remotelink | len 44
| 192.32.32.10 | remotelink | len 44
| 192.32.42.11 | remotelink | request SAM: inhibit+close target src ipaddr 192.32.42.11 expire 900
| 192.32.32.10 | remotelink | request SAM: inhibit+close target dst ipaddr 192.32.42.11 expire 900
| 192.32.42.11 | remotelink | len 44
| 192.32.42.11 | remotelink | len 44

From the console of the FireWall, you can view the connections table with the ‘fw tab’ command:

```
remotelink[admin]# fw tab -t sam_blocked_ips
localhost:
---------- sam_blocked_ips ----------
attributes: sync, keep

<c0202a0b; 00000006, 00040400, 00030300>
```

The IP Address of the blocked connection is given in Hex (c0202a0b=192.32.32.11)
Additionally, you can use the ‘fw sam’ commands to reconfigure the FireWall back to its original policy:

remoteink[admin]# fw sam
Usage:
sam [-v] [-s sam_server] [-t timeout] [-f fw_host] [-C] -n|-i|-I <criteria>
sam [-v] [-s sam_server] [-f fw_host] -D

options:
-v turn on verbose mode
-s sam_server the SAM server to be contacted. Default is localhost
-t timeout time in seconds for the inhibit operation. Default is never
-f fw_host the FireWalls to run the operation on. Should be either
   the name of a FireWalled object, the name of a group of
   FireWalled objects or one of the predefined names: All
   and Gateways. Default is All
-C cancel the specified operation
-n notify every time a connection that matches the specified
   criteria passes the firewall

operations:
-i inhibit connections that match the specified criteria
-I inhibit connections that match the specified criteria and
   close all existing connections that match it
-D delete all previous operations

criteria may be one of:
a. "src" <ip> match the source address of connections
b. "dst" <ip> match the destination address of connections
c. "any" <ip> match either the source or destination address of
   connections
d. "srv" <src ip> <dst ip> <service> <protocol>
   match specific source, destination and service

<ip>, <src ip> and <dst ip> may be a host name or a dotted notation address
<service> may be a service name (e.g. "telnet") or a service number
<protocol> may be a protocol name (e.g. "tcp") or a protocol number

examples:
1. For the next 20 seconds, notify when someone contacts www.checkpoint.com:
   sam -t 20 -n dst www.checkpoint.com
2. Inhibit 10.0.2.4 from accessing the WEB server on www.checkpoint.com:
   sam -i srv 10.0.2.4 www.checkpoint.com 80 6
3. Cancel the operation from example #2:
   sam -C -i srv 10.0.2.4 www.checkpoint.com 80 6
4. Have the SAM server on natasha.checkpoint.com cancel all previous SAM
   operations on the FireWall at frontline.us.checkpoint.com:
   sam -s natasha.checkpoint.com -f frontline.us.checkpoint.com -D