

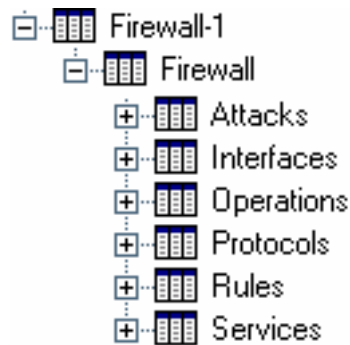
Check Point Firewall – 1™ Knowledge Module® for PATROL®



Introduction

According to this highly global World, basically in the business branch, the security is a very preponderant factor to become into a competitive group and not to dare the company actives where information is the key. At this context, Firewall-1 Knowledge Module for PATROL involves a vital echelon for the control and supervision of our firewall activity.

The monitoring spectre includes the analysis from the rules side, interfaces, protocols, services, operations audit and attacks detection. Everyone of the mentioned elements has a great variety of parameters with prepared and real time created information, formatted for an easy and complete understanding.



Automatic discovery

Check Point Firewall-1 Knowledge Module for PATROL has a powerful and flexible engine of discovering that allows us to detect the attacks and every kind of critical events every time that the firewall detects one. This way, the success degree of intrusion detection doesn't depend on the knowledge level of the administrators. Firewall-1 Knowledge Module discovers automatically the new danger situations obtained in the firewall with no need of making any anterior configuration in the Knowledge Module.



Attacks



Interfaces



Operations



Protocols



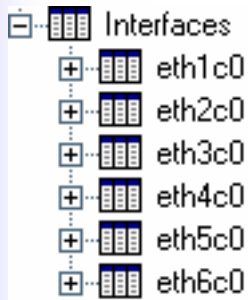
Rules



Services

Fundamental Objectives and Main Characteristics

Traffic analysis in Several Interfaces

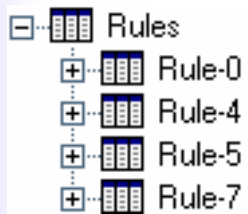


Automatic Discovery.

Check Point Firewall-1 Knowledge Module monitors the traffic absorbed for every firewall interface supervising the entry and exit transactions as well as the ones that have been accepted and denied. It includes the parameters that indicates the activity detected at every interface.



Traffic analysis by Rules

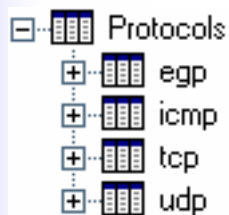


Automatic Discovery.

Supervision of the traffic from the used rules' side. Entry and exit Traffic's control as well as the accepted and denied transactions. It includes some parameters to indicate when the traffic runs through a rule.



Traffic analysis by Protocols

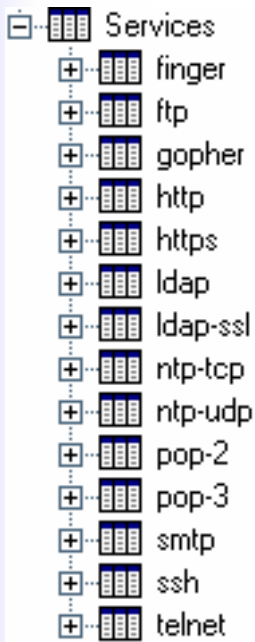


Automatic Discovery.


Traffic supervision from the used protocols side due to the entry and exit transactions. It includes some parameters indicating the activity for one protocol.

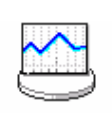


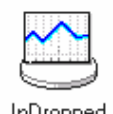
Traffic analysis by Services




Traffic supervision from the used services side due to the entry and exit transactions. It includes the parameters indicating the activity about one service.

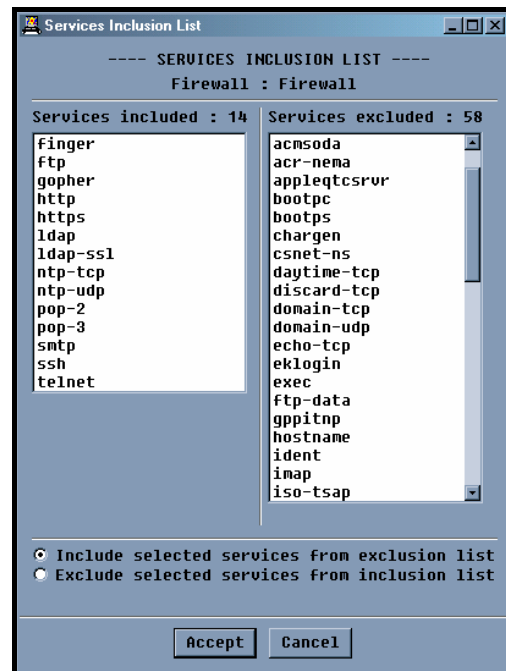

OutDropped


InAccepted


InDropped

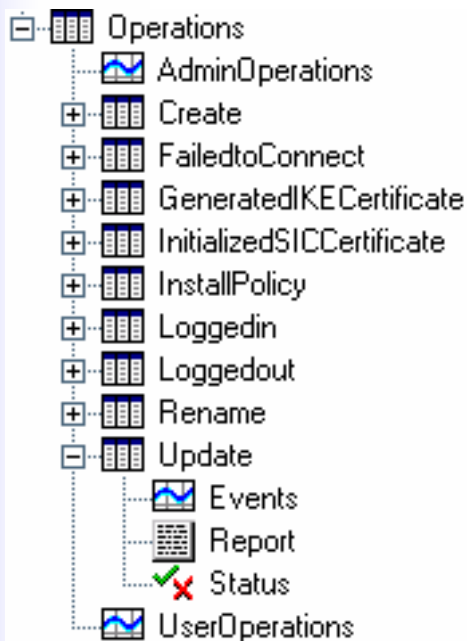

OutAccepted

Automatic Discovery .



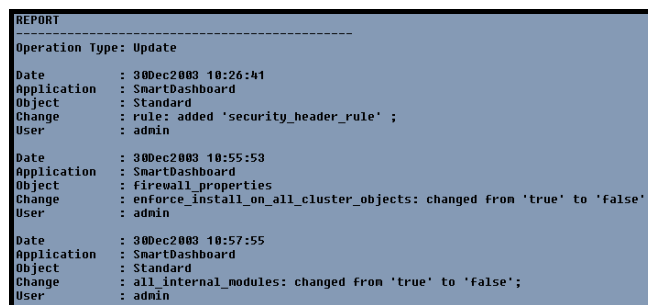
Services Inclusion List dialog box showing two columns: Services included (14) and Services excluded (58). Services included includes finger, ftp, gopher, http, https, ldap, ldap-ssl, ntp-tcp, ntp-udp, pop-2, pop-3, smtp, ssh, telnet. Services excluded includes acmsoda, acr-ena, appletcsrur, bootpc, bootps, chargen, csnet-ns, daytime-tcp, discard-tcp, domain-tcp, domain-udp, echo-tcp, eklogin, exec, ftp-data, gppitnp, hostname, ident, imap, iso-tsap. Radio buttons at the bottom allow for including or excluding selected services from the exclusion list.

Management Operations Audit



Real time discovery of the changes management about the firewall configuration. It detects new operations and it automatically includes them in the supervision. It shows in real time the realized management operation's details and it has the capability of storing that operations in the "annotations" field.

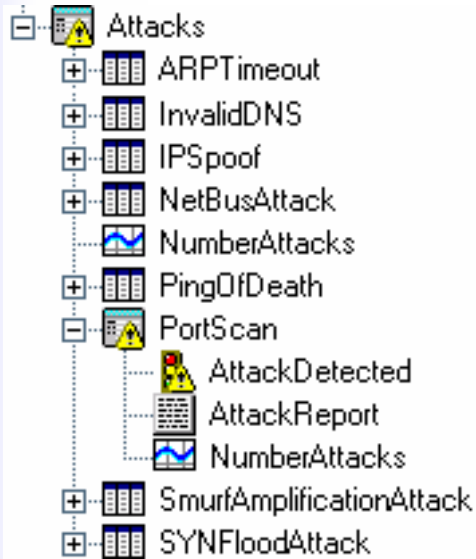
Automatic Discovery



```

REPORT
-----
Operation Type: Update
Date       : 30Dec2003 10:26:41
Application : SmartDashboard
Object     : Standard
Change    : rule: added 'security_header_rule' ;
User      : admin
Date       : 30Dec2003 10:55:53
Application : SmartDashboard
Object     : firewall_properties
Change    : enforce_install_on_all_cluster_objects: changed from 'true' to 'false';
User      : admin
Date       : 30Dec2003 10:57:55
Application : SmartDashboard
Object     : Standard
Change    : all_internal_modules: changed from 'true' to 'false';
User      : admin
    
```

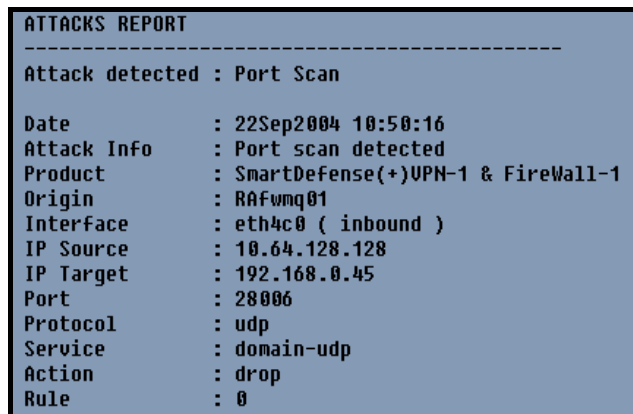
Attacks Detection



Automatic Discovery.

For Firewall-1 Knowledge Module is not needed any attack definition update. It automatically discovers any aggression intend that the firewall detects.

Check Point Firewall-1 Knowledge Module discovers in real time the new attacks and intrusion intends. You'll be informed about the external attacks and it will show you the reports about the suffered aggressions. You have the chance to archive every report by establishing the annotations parameters.



Supported Platforms

Check Point Firewall-1 Knowledge Module supports PATROL v3.5 or higher on platforms:

- Windows NT/2000/XP/2003
- Solaris SPARC version 2.7 or higher
- Linux : Red Hat, SuSE using Kernel 2.2x y 2.4x

Check Point Firewall-1 Knowledge Module works remotely on these platforms with support for Check Point Firewall-1 Next Generation (on Linux, Nokia, Solaris) :

Products	Technologies
<ul style="list-style-type: none"> - FireWall-1 NG Feature Pack (FP)1 - FireWall-1 NG FP 2 - FireWall-1 NG FP 3 with HotFix 1 	<ul style="list-style-type: none"> - Stateful Inspection - Application Intelligence - Web Intelligence - Malicious Code Protector - SMART - SecureXL

InnoTec System logos are registered trademarks in Spain and other selected countries.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc. Check Point, the Check Point logo, and FireWall-1 are registered trademarks or trademarks of Check Point Software Technologies Ltd. All other registered trademarks or trademarks belong to their respective companies.