

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

000c2921f8ab_fw... - 8.3.0 - Standalone Appliance

- ✓ **Licensing:** Expires in 23 days
- ✓ **Interfaces:** 2 of 10 enabled
- Admins logged in:** 2 administrators
- Application sessions:** 10
- VPN Definitions:** 0 (0 idle)
- Blackholed IPs:** 0
- Uptime:** 6 days
- Global Threat** Not in use

Messages from McAfee:

No messages are available

System Resources:

- User partition: 28%
0.3 of 1.0 GB used
- Root partition: 18%
29.9 of 158.4 MB used
- Memory usage: 30%
- CPU usage: 1%

Download updates:

Name	Version	Last checked
A/V signatures	5707	10/08/12 12:01 PM
Application signatures	3.158	10/08/12 12:01 PM
Geo-Location	200802120000.1	09/14/12 12:30 PM
IPS signatures	201004201202.2608	09/14/12 12:42 PM

Perform update(s)

Applications | Threats | Policy | Geo-Location | Users | GTI | NIA

Display the 15 most frequently-audited Network-Applications over the past day Go [Oct 14, 2012 to now]

Name	Count	Bytes transferred	Risk

Export View Audit...



Monitor Overview

Use the [Audit Viewing](#) area to view and filter audit output. Audits can be viewed for a set period of time or in real time and can be filtered using standard or customized filters.

Use the [Audit Management](#) area to configure audit log exporting, rolling, SSL signing, and other options. Audit logs can be exported in multiple formats via FTP and SCP. McAfee Firewall Reporter and syslog servers may be configured here.

Use the [ePolicy Orchestrator](#) area to configure a connection to a McAfee ePO server.

The [Firewall Policy Report](#) provides a comprehensive view of your firewall's policy configuration. The report is displayed using your default web browser.

Use the [Attack Responses](#) and [System Events Responses](#) to monitor your network for abnormal and potentially threatening activities, ranging from an attempted attack to an audit overflow. The Response Wizard allows you to create responses based on the audit event or attack, how frequently the audit occurs, and how the firewall will respond.

Use the [Profiler](#) area to send audit data to a McAfee Profiler server for analysis of policy and network traffic.

Use the [SNMP Agent](#) area to configure SNMP agent properties.

Ticket:

- Firewalls
 - Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

- Audits
- Common
 - All Audit
 - Attack All
 - Config Change
 - System All
 - VPN
 - Custom
 - Advanced
 - Access Control List
 - ACL Allow
 - ACL Deny
 - Application Defense Viol
 - Application Defense Viol
 - Attack Severe
 - Buffer Overflow Attack
 - Denied Authentication
 - DOS All
 - DOS Severe
 - Error
 - General Attack All
 - General Attack Severe
 - HA Failover
 - Hardware Software Fail
 - Host License Exceeded
 - IPFilter Deny
 - IPsec Error
 - Keyword Filter Failure
 - License Expiration
 - Log Overflow
 - Network Probe
 - Network Traffic
 - Not Config Change
 - Policy Violation All
 - Policy Violation Severe
 - Power Failure
 - Profiler Update Failure
 - Protocol Violation All
 - Protocol Violation Severe
 - Proxy Flood
 - Signature IPS Intrusion
 - Signature IPS Intrusion
 - Signature IPS Intrusion
 - Spam
 - Spam Severe
 - Syslog
 - System Critical
 - System Critical and Seve
 - TCP SYN Attack
 - Type Enforcement

Date	Time	Syslog	Type	Application	Source IP	Source Zone	Dest IP	Dest Zone	Info
2012-10-15	11:01:46 -0400	Debugging (7)	geninfo						Health Monitor data followsuptime_util: 6 days 23:03load_avg: 0.00...
2012-10-15	11:01:46 -0400	Debugging (7)	lcm						

Overview | Ascii | Filter Builder | IP Tools | Policy Tools

Date: _____ Time: _____ Syslog: _____ Facility: _____

Source: _____ Dest: _____

Info: _____

[diff](#)

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Audit Management | Firewall Reporter/Syslog

Audit Options

Show system statistics in audit log
 Require change ticket
 Create backups before each change ticket
Number of automatic backups to keep:

Logfile Options

Export Entry Name	Type	Summary
-------------------	------	---------

Export logfiles: disabled (35 minutes after every hour.)

Roll logfiles: daily at 2:00am.

Delete logs after export

Signature Options

Sign exported files
 Append signature to exported file Put signature in separate file
Sign with:

Ticket:

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator**
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Enable communication with ePO

IP Address:

Port:

User name:

Password:

Confirm password:

Cert authority:

Ticket:

- Firewalls
 - JPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report**
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Display Firewall Policy Report

The [Firewall Policy Report](#) provides a comprehensive view of your firewall's policy configuration. The report is displayed using your default web browser. You will need to enable JavaScript on your web browser to make full use of the report's features.



Policy Report from 000c2921f8ab_fwlocal.com

Name	Value
Configuration Source	000c2921f8ab_fwlocal.com
Creation Time	Mon Oct 15 11:09:35 2012
System Type	Standalone
System Version	8.3.0
Patches	8.3.0
Policy Version	2-1349712076



Policy

Access Control Rules

Name	Enabled	Action	Applications	Source Zones	Source	Destination Zones	Destination	Application Defense
Internet Services	<input checked="" type="checkbox"/>	allow	Internet Services	internal	all v4	external	all v4	minimal proxy
exclude_capability=; audit=standard; authenticator=none; authgroups=none; expire_time=; ipsresponse=none; nat_addr=localhost; nat_mode=normal; redir=none; redir_port=0; sign_category_grp=none; start_time=; timeperiod=all; ts_enable=no; ts_reputation=medium_unverified_threshold; ports=Default ports; Description: Allow Default Internet Services access from zone internal to zone external Last Changed By: system on Mon Oct 8 12:00:32 2012								
VoIP	<input type="checkbox"/>	allow	SIP, H.323	internal	all v4	external	all v4	minimal proxy
exclude_capability=; audit=standard; authenticator=none; authgroups=none; expire_time=; ipsresponse=none; nat_addr=localhost; nat_mode=normal; redir=none; redir_port=0; sign_category_grp=none; start_time=; timeperiod=all; ts_enable=no; ts_reputation=medium_unverified_threshold; ports=Default ports; Description: Allow VoIP access via SIP and H.323 from zone internal to zone external Last Changed By: system on Mon Oct 8 12:00:32 2012								
DNS	<input checked="" type="checkbox"/>							
Description: DNS resolver rules Last Changed By: system on Mon Oct 8 12:00:32 2012								
dnsp internal resolvers to external	<input checked="" type="checkbox"/>	allow	DNS	internal	internal primary DNS resolver	external	all v4	defaultgroup
exclude_capability=; audit=standard; authenticator=none; authgroups=none; expire_time=; ipsresponse=none; nat_addr=localhost; nat_mode=normal; redir=none; redir_port=0; sign_category_grp=none; start_time=; timeperiod=all; ts_enable=no; ts_reputation=medium_unverified_threshold; ports=Default ports; Description: Allow internal zone resolvers through to the external zone Last Changed By: system on Mon Oct 8 12:00:32 2012								
dnsp all to internal resolvers	<input checked="" type="checkbox"/>	allow	DNS	all	all v4	internal	internal primary DNS resolver	defaultgroup

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses**
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Attack Type	Frequency	Response
ACL Deny	ACL Deny	5 in 30 seconds	E-mail
Denied Authentication	Denied Authentication	20 in 60 seconds	E-mail
IPFilter Deny	IPFilter Deny	5 in 30 seconds	E-mail
IPS	Attack Severe	Every time	E-mail
Keyword Filter Failure	Keyword Filter Failure	5 in 30 seconds	E-mail
Network Probe	Network Probe	50 in 30 seconds	E-mail
Proxy Flood	Proxy Flood	5 in 10 seconds	E-mail, Blackhole
Signature IPS Intrusion All	Signature IPS Intrusion All	Every time	E-mail
Signature IPS Intrusion Blackholed	Signature IPS Intrusion Blackholed	Every time	E-mail, Blackhole
Signature IPS Intrusion Deny	Signature IPS Intrusion Deny	Every time	E-mail
Spam Filter Failure	Spam Severe	5 in 30 seconds	E-mail
TCP SYN Attack	TCP SYN Attack	Every time	E-mail
Type Enforcement	Type Enforcement	Every time	E-mail
Virus Filter Failure	Virus Severe	5 in 30 seconds	E-mail

New Modify Delete Disable

Response Settings

Ticket:

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses**
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Event Type	Frequency	Response
HA Failover	HA Failover	Every time	E-mail
Hardware Software Failure	Hardware Software Failure	Every time	E-mail, SNMP
Host License Exceeded	Host License Exceeded	Every time	E-mail
IPsec Error	IPsec Error	10 in 60 seconds	E-mail
License Expiration	License Expiration	Every time	E-mail
Log Overflow	Log Overflow	Every time	E-mail
Network Traffic	Network Traffic	1000 in 30 seconds	E-mail
Power Failure	Power Failure	Every time	E-mail
Profiler Update Failure	Profiler Update Failure	Every time	E-mail, SNMP
UPS System Shutdown	UPS System Shutdown	Every time	E-mail

New Modify Delete Disable

Response Settings

Ticket:

- Firewalls
 - jPk @ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler**
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Enable Profiler communication

Profiler IP:


Profiler common name (CN):

SCP username:

SCP password:

 The firewall will upload policies to the Profiler via SCP for analysis.

Profiler CA certificate: dn: CN=ca.n.lab, O=McAfee, C=US

 Please remember that you must use the certificate imported from Profiler.

[Advanced Options...](#)

Troubleshooting

- [Resynchronize Policy to Profiler](#) Force a policy upload to the Profiler after a loss of connection.
- [View Profiler Failure Audit](#) Display audit of failures of communication between the McAfee Firewall and Profiler.
- [View Profiler Network Traffic Audit](#) Display audit of network traffic between the McAfee Firewall and Profiler.

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Location:

Contact:

Enable authentication failure trap: Yes No

- Allowed Protocols
- SNMP v1
 - SNMP v2c
 - SNMP v3

Allowed get communities:

Community
public

New Modify Delete

SNMP v3 users:

User	Minimum security level	Auth Type	Privacy Protocol
------	------------------------	-----------	------------------

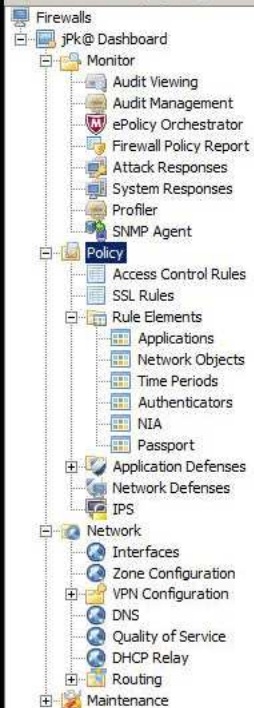
New Modify Delete

Trap version: v2c v3 settings

Trap destinations:

Host	Community
------	-----------

New Modify Delete



Policy Overview

Use the [Access Control Rules](#) area to manage access control rules which determine what traffic is allowed to pass through the firewall. Rules are the basis of your security policy.

Use the [SSL Rules](#) area to manage rules that determine what traffic is decrypted and possibly re-encrypted as it passes through the firewall.

Use the [Rule Elements](#) area to manage applications, network objects, authenticators, NIA, passport and time periods. These elements are essential components in access control rules.

Use the [Application Defenses](#) area to manage Application Defenses, application defense groups, Geo-Location database source and update settings, and virus scanning updates and advanced properties. These defenses are used in rules to provide advanced application-level inspection.

Use the [Network Defenses](#) area to control the audit output for suspicious lower-level traffic detected by the firewall when it automatically prevents that traffic from entering the firewall. Available protocols are TCP, IP, UDP, ICMP, ARP and IPsec.

Use the [IPS](#) area to configure the Intrusion Prevention System (IPS) response mappings and signature groups. These items are used in rules to inspect traffic for known network-based attacks.

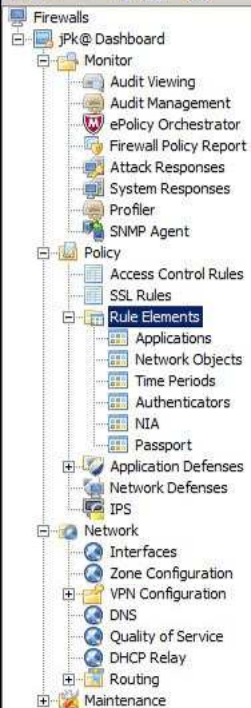
- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules**
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Enabled	Act...	Application	Source Zone	Source	Destination Z...	Destination	Application Defense	Authentication	Ports	Description	IPS Sig...
<ul style="list-style-type: none"> (1-9) Firewall Policy (1) Internet Serv (2) VoIP (3-4) DNS (3) dnsp intern (4) dnsp all to i (5-8) Administratic (5) SmartFilter (6) Login Cons (7) Admin Cons (8) Secure She (9) Deny All 												
(1) Internet Serv	Allow		Internet Services (Gro	internal	<Any V4>	external	<Any V4>	minimal proxy			Allow Default Internet Services access from zone internal to zone external	
(2) VoIP	Allow		SIP H.323	internal	<Any V4>	external	<Any V4>	minimal proxy		TCP/1720 UDP/1719 UDP/5060	Allow VoIP access via SIP and H.323 from zone internal to zone external	
<ul style="list-style-type: none"> (3-4) DNS (3) dnsp intern (4) dnsp all to i 												
(3) dnsp intern	Allow		DNS	internal	internal primary DI	external	<Any V4>	<Default group>		TCP/53 UDP/53	Allow internal zone resolvers through to the external zone	
(4) dnsp all to i	Allow		DNS	<Any>	<Any V4>	internal	internal primary DI	<Default group>		TCP/53 UDP/53	Allow dns clients in all zones through to the internal zone resolvers	
<ul style="list-style-type: none"> (5-8) Administratic (5) SmartFilter (6) Login Cons (7) Admin Cons (8) Secure She 												
(5) SmartFilter	Allow		SmartFilter Admin Con	<Any>	<Any V4>	<Any>	<Any V4>	<Default group>		TCP/9013	Allow access for firewall administration.	
(6) Login Cons	Allow		Login Console	Firewall	<Any V4>	Firewall	<Any V4>	<Default group>	Password		Allow login from system console.	
(7) Admin Cons	Allow		Admin Console	internal	<Any V4>	internal	<Any V4>	<Default group>	Password	TCP/9003	Allow Admin Console access from the internal zone	
(8) Secure She	Allow		SSH Server	internal	<Any V4>	internal	<Any V4>	<Default group>	Password	TCP/22	Allow SSH server access from the internal zone	
(9) Deny All	Deny		<Any>	<Any>	<Any>	<Any>	<Any>	<Default group>			Deny access from any zone to any zone.	

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules**
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Find: Clear Columns

Name	Enabled	Action	Type	Source Zone	Source	User	Port	Destination ...	Destination	Description
(1-1) SSL Policy										
(1) Exempt All	✓	No decryption	<Any>	<Any>	<Any>		<Any>	<Any>	<Any>	



Rule Elements Overview

Use the [Applications](#) area to view, create, and group applications. Applications are used in access control rules to identify the network applications associated with connections.

Use the [Network Objects](#) area to configure domain, Geo-Location, host, IP address, IP range, netmap, and subnet objects. Objects are then used in rules to determine a rule's source and destination.

Use the [Passport](#) area to configure interaction with Microsoft Logon Controller (MLC) servers and other aspects of the firewall's single sign on service.

Use the [Authenticators](#) area to manage Passport (single sign on), password, LDAP, RADIUS, and Windows authenticators. Authenticators are used in rules to validate a person's identity before he or she is allowed to log into a network server.

Use the [NIA](#) area to configure interaction with the Network Integrity Agents (NIA). NIAs provide per connection information to the firewall to aid in policy decision-making.

Use the [Time Periods](#) area to configure continuous and recurring time segments. Time periods are used in rules to determine the days and times that a rule is active.

Firewalls

- Dashboard
- Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
- Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Manage: Applications

Filter by risk:
 LOW MEDIUM HIGH

Filter by categories:
 To filter applications by category, click on one or more categories from the list below.

- Anonymizers/Proxies
- Authentication Services
- Business Web Applications
- Collaboration/Content Management
- Commercial Monitoring
- Database
- Directory Services
- ERP/CRM
- Email
- Email Harvesters
- Embedded Web Applications
- Feed Readers
- File Sharing
- Gaming
- IT Utilities
- Infrastructure Services
- Instant Messaging
- Mobile Software
- Offline Crawlers
- Peer to Peer (P2P)
- Photo/Video Sharing
- Remote Administration
- Remote Desktop/Terminal Services
- Search/Indexing Engine Spiders and Crawlers
- Social Networking
- Software/System Updates
- Storage
- Streaming Media
- Toolbars/PC Utilities
- Tunnels
- Voice over IP (VoIP)
- Web Browsing
- Web Conferencing
- Web Mail

1432 Matching Application(s)

Risk	Name	Filtered Categories	Other Categories
HIGH	100bao		Peer to Peer (P2P)
LOW	123spider		Search/Indexing Engine Spiders and Crawlers
LOW	126 Mail		Web Mail
LOW	1fichier		Storage
LOW	1und1 Mail		Web Mail
LOW	2Bone		Offline Crawlers
HIGH	2channel		Social Networking
LOW	2DPlay		Gaming
HIGH	4FileHosting		File Sharing
LOW	4RemoteSupport		Remote Administration
HIGH	4shared		File Sharing
HIGH	51.com		Gaming, Social Networking, Storage, Streaming Media
LOW	9cast.net		Streaming Media
HIGH	<Any>		Infrastructure Services

Name: 100bao Risk: HIGH

Application discovery (last 180 days):
 No stats available at this time.

Categories: Peer to Peer (P2P)

Associated rules:

Action	Name

Description:
100bao: A peer-to-peer file-sharing application
 Ports: TCP/80,443,1234 SSL/443
[McAfee](#) [Audit](#) [Google](#) [Bing](#)

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects**
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Find:

Groups Object In

Type	Name	Value	Description
IP Address	internal primary DNS resolver	192.168.1.254	Network object for internal zone primary DNS resolver

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods**
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Find:

Name	Days and Times	Description
Business Hours	Mon - Fri, 8:00 AM - 5:00 PM	
Weekdays	Mon - Fri, All day	
Weekends	Sat - Sun, All day	

Name:

Description:

Days and Times

Mon - Fri, 8:00 AM - 5:00 PM

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators**
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Type	Properties	Description
Password	Password		Static password authenticator

Name: Password Type: Password Description: Static password authenticator

General

Login settings

Login prompt: Username:

Password prompt: Password:

Expiration message: Your password has expired.

Password expiration: 90 days

Password requirements


Minimum Password Length: 8

Allow simple passwords (AlphaNumeric)

Require complex passwords

Require 2 of the four character groups in every password.

Require at least 2 characters(s) per required group in every password

 The four character groups are: lowercase letters, uppercase letters, numbers, and special characters such as #.

Example valid password: abcd0123

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA**
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

NIA | Hosts and Discovery | **Advanced Settings**

Enable NIA

NIA Settings

Shared Key:

Authentication: Enable Mode:

CA Certificate:

FW Certificate:

Check Certificate Revocation

Allow Unknown Revocation

Allow Expired Certificate

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Static Passport authenticator

Manage Passports

General | Advanced

Establish passport credentials

Passive (MLC)

IP address:

Test MLC Connection

Certificate:

Active

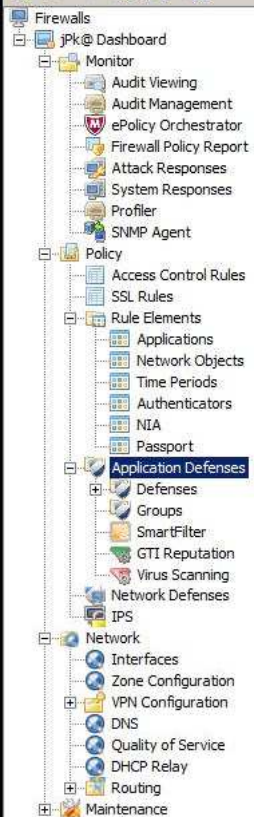
Authentication mode

- Inband
- Web login
- Web login with active session mode

Authenticators used to establish Passport credentials:

- Password

Default authenticator:



Application Defenses Overview

Use the [Defenses](#) area to configure advanced properties for specific applications. These items are used in rules to implement various connection permissions, scanning, and filtering.

Use the [Application Defense Groups](#) area to select a defense for each category (for example, HTTP, FTP, SNMP) to include in an application defense group. These groups are often used in rules that use service groups.

Use the [SmartFilter](#) area to configure the ways in which the firewall interacts with local or remote SmartFilter services.

Use the [GTI Reputation](#) area to configure the Global Threat Intelligence threshold. Global Threat Intelligence is a reputation service that filters incoming connections and provides a reputation score.

Use the [Virus Scanning](#) area to configure the anti-virus signature file download properties and advanced scanner properties. Virus scanning is an add-on module and must be licensed before the firewall will download the signature files. Apply spam filtering to rules using the HTTP, Mail (Sendmail), and FTP Application Defenses.

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T 120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Description
connection settings	This is a default Application Defense configured to provide connection settings (timeouts).
minimal proxy	This is a default Application Defense that is configured to force sessions through a proxy without additional enforcements.

New Modify Rename Delete Set Expected Connections Usage Duplicate

Name: Description:

General Stateful Inspection Other IP Filter Settings

- Use TCP proxy
- Use UDP proxy
- Use ICMP proxy

Selection of the above values will force applications to run through the firewall's proxies.

Timeout values:

Agent Name	Timeout	Value (in secs)
Active Passport	TCP idle	7200
Admin Console	TCP idle	0
Change Password Server	TCP idle	1800
Cluster Registration	TCP idle	7200
CommandCenter	TCP idle	7200
Common Access Card	TCP idle	60
DNS	UDP idle	60
DNS	TCP idle	3600
Enterprise Relay Server	TCP idle	7200
FTP	TCP connect	15
FTP	TCP idle	7200
H323	UDP idle	60
H323	TCP idle	7200
HTTP	TCP connect	15
HTTP	TCP idle	60
ICA	UDP idle	60
ICA	TCP idle	3600
IIOIP	TCP idle	3600
MSSQL	TCP idle	7200
Non-TCP UDP Protocols	response	15
Oracle	TCP idle	7200
RealMedia	UDP idle	3600
RSH	TCP idle	7200
RTSP	UDP idle	3600
SIP	UDP idle	60
SmartFilter Admin Console	TCP idle	7200
SmartFilter Redirect Server	TCP idle	7200
SMTP	TCP idle	7200
SNMP	UDP idle	60
SOCKS	UDP idle	30
SOCKS	TCP idle	7200
SSH	TCP idle	7200

Advanced

Firewalls

- jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Description	Type	HTTP URL control	FTP URL control	HTTP request	HTTP reply	MIME/Virus/Spyware	Content control	SmartFilter	Relaxed enforcements	Upstream proxy
Anti-Virus Scanning	Anti-Virus Scanning HTTP application defense	Combined	Off	Off	Off	Off	On	Off	Off	Client and Server	Off
minimal proxy	minimal proxy HTTP application defense	Combined	Off	Off	Off	Off	Off	Off	Off	Client and Server	Off
Trusted Inbound HTTP	Used for trusted inbound HTTP connections that ...	Server	On	On	On	On	Off	On	Off	Off	Not Applicable
URL Filtering	URL Filtering HTTP application defense	Combined	Off	Off	Off	Off	Off	Off	On	Client and Server	Off
URL Filtering and Anti-Virus Scanning	URL Filtering and Anti-Virus Scanning HTTP applic...	Combined	Off	Off	Off	Off	On	Off	On	Client and Server	Off

New Modify Rename Delete

URL Translation Rules Usage Duplicate

Name: Anti-Virus Scanning Type: Combined Description: Anti-Virus Scanning HTTP application defense

Enforcements | HTTP URL control | FTP URL control | HTTP request | HTTP reply | MIME/Virus/Spyware | Content control | SmartFilter | Connection

HTTP client and server enforcements

- HTTP URL control
- FTP URL control
- HTTP request
- HTTP reply
- MIME/Virus/Spyware
- Content control
- SmartFilter

Relax protocol enforcements: Client and Server

Rewrite Microsoft OWA HTTP
(Applies to HTTPS. Valid only when the 'SSL Rules' rule action is set to 'Decrypt Only'.)

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Description	Media Filtering	Media Filters
minimal proxy	minimal proxy sip application defense.	Not Enforced	Audio, Video

New Modify Rename Delete Usage Duplicate


Name: minimal proxy Description: minimal proxy sip application defense.

General Media Filters

Enforce Media Filtering
Maximum Call Duration: 86400 seconds

Peer Types

- The SIP peers must be user agents (e.g., phones)
This option is the most restrictive.
- The SIP peers can be routers (intermediaries that negotiate calls on behalf of user agents)
This option is the least restrictive.

 Some routers masquerade as user agents. See the McAfee Firewall Enterprise product documentation for more information.

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Description
minimal proxy	minimal proxy ssh application defense.

New Modify Rename Delete SSH Known Hosts Usage Duplicate

Name: minimal proxy Description: minimal proxy ssh application defense.

Channels Client Authentication Client Advanced Server Advanced

Allow remote shell execution
 Allow remote command execution (includes SCP)
 Allow X11 forwarding

Port forwarding (tunneling)
 Allow local port forwarding
 Allow remote port forwarding

Allowed SFTP operations
 None
 Any
 Selected from list

- Change attributes of files on the server
- Create directories on the server
- Create files on the server
- Delete directories on the server
- Delete files on the server
- Read directories on the server
- Read files on the server
- Rename files on the server
- Write files on the server

Allowed non-SFTP subsystems
 None
 Any
 Specified in list

New Delete

- Firewalls
 - jkp@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOp
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Name	Description	Generic	Citrix	FTP	H.323	HTTP	IIOp	Mail	SMTP	Oracle	SIP	SNMP	SOCKS
Anti-Virus Scanning	This is a default Application Defense group config...	minimal pr...	minimal pr...	Anti-Virus...	minimal pr...	Anti-Virus...	minimal pr...	Anti-Virus...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...
connection settings	This is a default Application Defense grou...	connecti...	<None>	<None>	<None>	<None>	<None>	<None>	<None>	<None>	<None>	<None>	<None>
minimal proxy	This is a default Application Defense group that i...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...
URL Filtering	This is a default Application Defense group confi...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	URL Filter...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...
URL Filtering and Anti-Virus Scanning	This is a default Application Defense group confi...	minimal pr...	minimal pr...	Anti-Virus...	minimal pr...	URL Filter...	minimal pr...	Anti-Virus...	minimal pr...	minimal pr...	minimal pr...	minimal pr...	minimal pr...

Name: Description:

Select the Application Defenses for this group:

Application Defense	Name
Generic (Required)	minimal proxy
Citrix	minimal proxy
FTP	Anti-Virus Scanning
H.323	minimal proxy
HTTP	Anti-Virus Scanning
IIOp	minimal proxy
Mail (Sendmail)	Anti-Virus Scanning
Mail (SMTP proxy)	minimal proxy
Oracle	minimal proxy
SIP	minimal proxy
SNMP	minimal proxy
SOCKS	minimal proxy
SSH	minimal proxy
T120	minimal proxy

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

SmartFilter Management | Filter Policies | Custom | Audit

Categories:

Find:

Category Name
School Cheating Information
Search Engines
Sexual Materials
Shareware/Freeware
Software/Hardware
Spam URLs
Sports
Spyware/Adware/Keyloggers
Stock Trading
Streaming Media
Technical Information
Technical/Business Forums
Text/Spoken Only
Tobacco
Travel
Usenet News
User Defined Category 0
User Defined Category 1
User Defined Category 2
User Defined Category 3
User Defined Category 4
User Defined Category 5
User Defined Category 6
User Defined Category 7
User Defined Category 8
User Defined Category 9
Violence
Visual Search Engine
Weapons
Web Ads
Web Mail
Web Phone

Custom Web Mail sites:

Find:

URL

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Global Threat Intelligence Whitelist

Do not perform GTI on:

- IP Address objects
- IP Range objects
- Subnet objects
- Host objects
- Zones except the following:

[Add]

Do not perform GTI on these objects:

[Empty list box]

Edit

Audit

Audit traffic allowed by GTI

Tools

Query reputation at trustedsource.org:

Host: [Query]

Global Threat Intelligence Filtering

Perform GTI filtering on inbound mail

Reputation threshold:

Advanced Settings

Adjust reputation boundaries:

Low Risk Unverified Medium High Risk

(-255 to 14) (15 to 29) (30 to 49) (50 to 255)



Default reputation if GTI servers are unavailable:

Restore Defaults

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Scanning Distribution

(Configure the number of scanners to run concurrently for files in each size range)

File Size Range	Scanners
Up to 40K	2
Up to 100K	2
Up to 1M	1
Unlimited	1

Modify

Scan Buffer Size (KB): (Recommended: 50 KB, Maximum: 64 KB)

Archive Scan Buffer Size (MB): (Recommended: 128 MB, Maximum: 512 MB)

Maximum Number of Files to Scan in an Archive:

Scan Encrypted Files

Firewalls

- jPk@ Dashboard
- Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
- Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Orade
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Select the attacks and protocol compliance issues to audit. The McAfee Firewall Enterprise always defends against all attacks and compliance issues regardless of the audits you select.

Restore Defaults

TCP | IP | UDP | ICMP | ARP | IPsec | IPv6

TCP Audits

Audit the selected TCP attacks:

- aborted connection attempt
- crafted packet probe
- forged source address
- invalid offset
- invalid sequence on SYN-ACK
- LAND DOS attack
- out of window RST
- RST with no data transferred
- SYN flood
- syn hijack on active connection
- SYN with FIN scan
- SYN-ACK probe

Audit the selected TCP compliance issues:

- Audit all TCP compliance issues
- Audit severe and moderate TCP compliance issues
- Audit severe TCP compliance issues
- Do not audit any TCP compliance issues

Select All Deselect All

TCP Audit Frequency

Limit auditing (recommended)

Audit the first 1 occurrence(s) every 1 seconds.

Always audit

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOp
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Orade
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Response Mappings | Signature Groups | Signature Browser

Find:

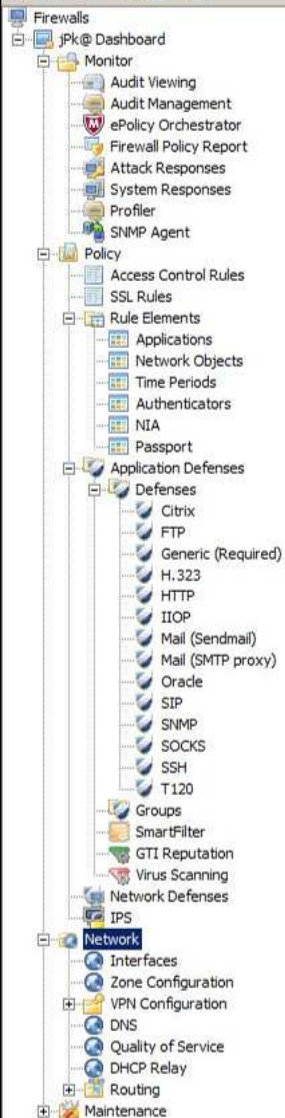
Name	Description	Class Types
default	Factory provided response m...	IDS:BACKDOOR, IDS:CHECK-BD, IDS:CHECK-EX, IDS:COMPONENT, IDS:CONFIRMED, IDS:DECOY, IDS:DISCOVER, IDS:DOS, IDS:EMPTY, IDS:FILE, IDS:POLICY, IDS:REXPLOIT, IDS:SUSPECT, IDS:UEXPLOIT, IDS:WORM, IPS:BACKDC...

Name:

Description:

Class Types:

Name	Type	Response	Duration (s)	Description
Backdoor Activity	IDS	Allow	0	Communication is likely associated with an active backdoor
Backdoor Activity	IPS	Drop	0	Communication is likely associated with an active backdoor
Backdoor Check	IDS	Allow	0	Communication is designed to check for a backdoor. This can be part of an attack, or attacker is looking for a well known backdoor that might have been part of someone else's attack.
Backdoor Check	IPS	Drop	0	Communication is designed to check for a backdoor. This can be part of an attack, or attacker is looking for a well known backdoor that might have been part of someone else's attack.
Component	IDS	Allow	0	Is part of an attack, but whose purpose is undeterministic. Must notable is shellcode
Component	IPS	Drop	0	Is part of an attack, but whose purpose is undeterministic. Must notable is shellcode
Confirmed attack	IDS	Allow	0	Presence of vulnerability and exploit appear in same session.
Confirmed attack	IPS	Drop	0	Presence of vulnerability and exploit appear in same session.
Decoy	IDS	Allow	0	Normal activity. Signatures are not to be used for IDS, firewalls or IPS.
Decoy	IPS	Drop	0	Normal activity. Signatures are not to be used for IDS, firewalls or IPS.
Denial of Service	IDS	Allow	0	Attacks targeting to disable normal service by consuming too much resources
Denial of Service	IPS	Drop	0	Attacks targeting to disable normal service by consuming too much resources
Discovery	IDS	Allow	0	Communications are used to discover systems, services and applications.
Discovery	IPS	Drop	0	Communications are used to discover systems, services and applications.
Exploit Check	IDS	Allow	0	Exploit checks are attacks that check to see if a system has a given exploit. These attacks by themselves do not exploit the system, and require a follow-on attack
Exploit Check	IPS	Drop	0	Exploit checks are attacks that check to see if a system has a given exploit. These attacks by themselves do not exploit the system, and require a follow-on attack
File Identification	IDS	Allow	0	This signature identifies a file or file attribute.
File Identification	IPS	Drop	0	This signature identifies a file or file attribute.
No Data	IDS	Allow	0	Packet had no data. Likely negotiation packet
No Data	IPS	Drop	0	Packet had no data. Likely negotiation packet
Policy	IDS	Allow	0	Activity is not consistent with good security practices
Policy	IPS	Drop	0	Activity is not consistent with good security practices
Root Level Exploit	IDS	Allow	0	root level exploit alarm is associated with attacks that have the capability of gaining the highest level access of the system
Root Level Exploit	IPS	Drop	0	root level exploit alarm is associated with attacks that have the capability of gaining the highest level access of the system
Suspicious	IDS	Allow	0	Activity is normally assoctaed with malicious or policy violations, but has a degree of false positives not meeting FirstLight standards
Suspicious	IPS	Drop	0	Activity is normally assoctaed with malicious or policy violations, but has a degree of false positives not meeting FirstLight standards
User Level Exploit	IDS	Allow	0	User level exploits allow an attacker to gain minimal level of access (or increased level) to the system. They do not however grant complete access to the system.
User Level Exploit	IPS	Drop	0	User level exploits allow an attacker to gain minimal level of access (or increased level) to the system. They do not however grant complete access to the system.
Worms and Viruses	IDS	Allow	0	These communications are associated directly with worms and viruses
Worms and Viruses	IPS	Drop	0	These communications are associated directly with worms and viruses
Backdoor Activity	POLICY	Allow no Audit	0	Communication is likely associated with an active backdoor
Backdoor Check	POLICY	Allow no Audit	0	Communication is designed to check for a backdoor. This can be part of an attack. or attacker is looking for a well known backdoor that might have been part of someone else's attack.



Network Overview

Use the [Interfaces](#) area to manage the firewall's network interface cards and VLAN-enabled interfaces.

Use the [Zone Configuration](#) area to configure the type-enforced network areas that are to be treated the same from a policy perspective.

Use the [VPN Configuration](#) area to manage the VPN definitions that provide network-extending secure data transmissions to and through the firewall, and the client address pools that can provide internal IP addresses to external VPN clients.

Use the [DNS](#) area to configure DNS files when using firewall-hosted DNS. (You should either edit DNS files using the Admin Console or using a file editor, but not both. Alternating methods may cause your changes to be overwritten.)

Use the [Quality of Service](#) area to configure Quality of Service (QoS) profiles. QoS profiles consist of queues with assigned bandwidth and priority.

Use the [DHCP Relay](#) area to configure DHCP Relay addresses and other configuration properties.

Use the [Routing](#) area to configure static routing and dynamic routing (BGP, OSPF, OSPF IPv6, PIMSM, and RIP).

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOp
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T 120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Interface Configuration | NIC and NIC Group Configuration

Find:

Show Status

Name	NIC Or NIC Group	Enabled	Zone	IP addresses	Description
<Not in use>	em2				
<Not in use>	em3				
<Not in use>	em4				
<Not in use>	em5				
<Not in use>	em6				
<Not in use>	em7				
<Not in use>	em8				
<Not in use>	em9				
external_network	em0	✓	external	192.168.2.250	Default external network interface
internal_network	em1	✓	internal	192.168.1.250	Default internal network interface

Additional interface information:

NIC or NIC Group: em2

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Internet Zone: external

Name	Groups	Description
external - Internet zone		
internal		

Zone name: external

Description: ID: 1

Groups

Connection Options

- Application discovery
- Honor ICMP redirect
- Respond to ICMP echo and timestamp
- Hide port unreachables

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration**
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance



VPN Configuration Overview

Use the [VPN Definitions](#) area to configure all of the elements of a VPN connection. These elements include the VPN's source and destination, the remote and local authentication methods, what encryption and authentication algorithms to use, and advanced properties such as IKE and rekey settings.

Use the [Client Address Pools](#) area to manage IP address pools that can provide internal IP addresses to external VPN clients.

Use the [ISAKMP Server](#) area to manage configuration for the ISAKMP server.

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T 120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server**
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Configure the Internet Security Association and Key Management Protocol (ISAKMP) server, which generates and exchanges keys for VPN sessions.

Audit Level:

Advanced ISAKMP Server Options

Adjust the connection and retransmission timeouts, limit the number of new connections to the ISAKMP server, or disable certificate negotiation.

XAUTH (Extended Authentication) Configuration

Allowed XAUTH Methods:

Password

Default XAUTH Method:

Limit the number of active VPNs to one per user or adjust the connection and retransmission timeouts of XAUTH challenges.

- Firewalls
 - jPk@ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Maintenance

Find:

Profile Name	Description
--------------	-------------

Load QoS Policy QoS Status

Profile name: Remaining bandwidth:

Description:

Find:

Queue Name	Priority	Allocated Bandwidth	Ports	Can Borrow	Description
------------	----------	---------------------	-------	------------	-------------

- Firewalls
 - JKP @ Dashboard
 - Monitor
 - Audit Viewing
 - Audit Management
 - ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
 - Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T 120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
 - Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Static Routing
 - Dynamic Routing
 - Maintenance




Routing Overview

Use the [Static Routing](#) area to configure the firewall's default route and any other necessary static routes.

Use the Dynamic Routing area to configure dynamic routing using [BGP](#), [OSPF](#), [OSPF IPv6](#), [PIMSM](#), and [RIP](#). BGP, OSPF, and RIP can also be configured by connecting via Telnet to the protocol's respective server. PIMSM can also be configured by using the command line tool xorsh.

- ePolicy Orchestrator
 - Firewall Policy Report
 - Attack Responses
 - System Responses
 - Profiler
 - SNMP Agent
- Policy
 - Access Control Rules
 - SSL Rules
 - Rule Elements
 - Applications
 - Network Objects
 - Time Periods
 - Authenticators
 - NIA
 - Passport
 - Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOp
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Static Routing
 - Dynamic Routing
 - BGP
 - OSPF
 - OSPF IPv6
 - PIMSM
 - RIP
- Maintenance

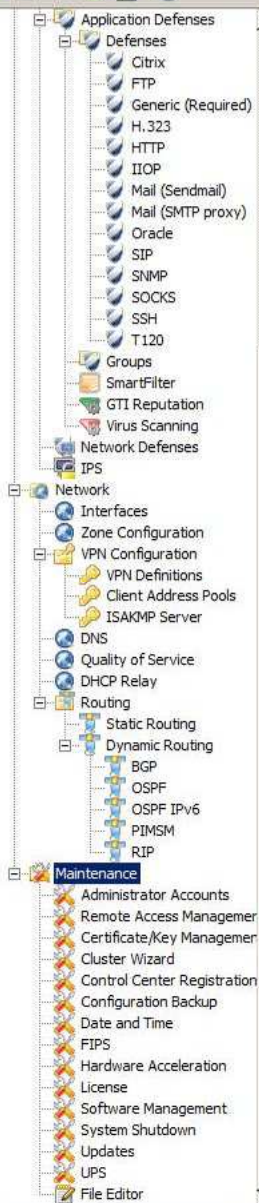
Configuration file:

 The BGP service will be automatically restarted when the configuration file is saved.

Compare running configuration to configuration file

- Compare running configuration to starting configuration
- Show all BGP neighbors
- Show all BGP summary neighbors
- Show IPv4 BGP routes
- Show IPv6 BGP routes
- Show IPv6 BGP summary neighbors
- Show running configuration
- Show starting configuration

Overwrite configuration file with running configuration:



Firewall Enterprise

Copyright © 1995-2012 McAfee, Inc. All rights reserved.

Maintenance Overview

Use the [Administrator Accounts](#) area to manage accounts for administrators who have access to this firewall.

Use the [Remote Access Management](#) area to configure settings for the Admin Console server and the SSH server on the firewall.

Use the [Certificate/Key Management](#) area to manage certificates for remote authentication. You can create, modify, import, and export self-signed certificates, Certificate Authorities, and SSL certificates, as well as configure the certificate server.

Use the [Cluster Wizard](#) to create or join a High Availability cluster.

Use the [Control Center Registration](#) area to register this firewall with a Control Center management server.

Use the [Configuration Backup](#) area to manage backing up and restoring configuration files. You can back up your firewall configuration information to a client system (where the Admin Console is installed), to another firewall, or to this firewall's hard drive.

Use the [Date and Time](#) area to set the firewall's system clock to the correct date and time. You can also configure the use of Network Time Protocol (NTP) servers here.

Use the [FIPS](#) area to enforce US Federal Information Processing Standard 140-2.

Use the [Hardware Acceleration](#) area to configure cryptographic accelerators.

Use the [License](#) area to update your firewall license and to view and delete the hosts that count against the license host limit. You can also enter company contact information.

Use the [Software Management](#) area to manage software patches. You can download, install, uninstall, and roll back patches.

Use the [System Shutdown](#) area to reboot or power down the firewall. You can shut down the firewall immediately or schedule a delayed shut down.

Use the [Updates](#) area to manage updates for A/V signatures, Application signatures, Geo-Location, IPS signatures, Message board and SmartFilter.

Use the [UPS](#) area to configure an uninterruptible power supply.

Use the [File Editor](#) to view and edit files located on your firewall.

Configuration Backup | Configuration Restore | Schedule

Backup McAfee Firewall Enterprise Configuration

- Client system
- Local McAfee Firewall Enterprise
- Remote system (SCP)

Username:

Password:


Hostname: Port:

Directory:

Backup Now

Disaster Recovery Backup

Create Disaster Recovery Backup

 You must connect a USB flash drive to the appliance before initiating this backup. A disaster recovery backup includes the current configuration and installed patches. This backup can only be restored during the re-imaging process.

Manage McAfee Firewall Enterprise Configuration Backups

Current local configuration backups:

Name	Version	Date	Location	Type	Ticket	Summary
initial_configuration	8.3.0	Oct 08 2012 10:C...	Local Disk	Complete		Host: 000c2921f8ab_fwlocal.com, System type: SA, Packages: 8.3.0



Delete Upload Download Compare Audit

Refresh

- Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOIP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
 - Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Static Routing
 - Dynamic Routing
 - BGP
 - OSPF
 - OSPF IPv6
 - PIMSM
 - RIP
- Maintenance
 - Administrator Accounts
 - Remote Access Manager
 - Certificate/Key Manager
 - Cluster Wizard
 - Control Center Registration
 - Configuration Backup
 - Date and Time
 - FIPS
 - Hardware Acceleration
 - License
 - Software Management
 - System Shutdown
 - Updates
 - UPS
 - File Editor

- Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
- Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Static Routing
 - Dynamic Routing
 - BGP
 - OSPF
 - OSPF IPv6
 - PIMSM
 - RIP
- Maintenance
 - Administrator Accounts
 - Remote Access Manager
 - Certificate/Key Manager
 - Cluster Wizard
 - Control Center Registration
 - Configuration Backup
 - Date and Time
 - FIPS
 - Hardware Acceleration**
 - License
 - Software Management
 - System Shutdown
 - Updates
 - UPS
 - File Editor

Hardware Accelerators:

Device Name	SSL Acceleration	Enabled
intel	RSA, CIPHERS, DIGESTS	off

- Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
- Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Static Routing
 - Dynamic Routing
 - BGP
 - OSPF
 - OSPF IPv6
 - PIMSM
 - RIP
- Maintenance
 - Administrator Accounts
 - Remote Access Manager
 - Certificate/Key Manager
 - Cluster Wizard
 - Control Center Registration
 - Configuration Backup
 - Date and Time
 - FIPS
 - Hardware Acceleration
 - License
 - Software Management
 - System Shutdown
 - Updates
 - UPS
 - File Editor

Enable Uninterruptible Power Supply (UPS)

UPS Serial Port: COM1

Battery Time: 900 (seconds)

- Application Defenses
 - Defenses
 - Citrix
 - FTP
 - Generic (Required)
 - H.323
 - HTTP
 - IIOP
 - Mail (Sendmail)
 - Mail (SMTP proxy)
 - Oracle
 - SIP
 - SNMP
 - SOCKS
 - SSH
 - T.120
 - Groups
 - SmartFilter
 - GTI Reputation
 - Virus Scanning
- Network Defenses
 - IPS
- Network
 - Interfaces
 - Zone Configuration
 - VPN Configuration
 - VPN Definitions
 - Client Address Pools
 - ISAKMP Server
 - DNS
 - Quality of Service
 - DHCP Relay
 - Routing
 - Static Routing
 - Dynamic Routing
 - BGP
 - OSPF
 - OSPF IPv6
 - PIMSM
 - RIP
- Maintenance
 - Administrator Accounts
 - Remote Access Manager
 - Certificate/Key Manager
 - Cluster Wizard
 - Control Center Registration
 - Configuration Backup
 - Date and Time
 - FIPS
 - Hardware Acceleration
 - License
 - Software Management
 - System Shutdown
 - Updates
 - UPS
 - File Editor

WARNING:

Only experienced administrators should attempt to manually edit configuration files.

Changes made will not be checked for errors.

Start File Editor