McAfee®

Application Note

Protecting Industrial Control Systems Using McAfee Firewall Enterprise (*Sidewinder*®)

This document describes how to configure McAfee Firewall Enterprise to provide highly secure protection for critical control systems for utility, power, energy, water, chemical, and manufacturing industries.

In this document ...

About this document

This document describes how to configure McAfee Firewall Enterprise *(Sidewinder)* to provide secure protection for critical control systems for utility, power, energy, water, chemical, and manufacturing industries. It includes configuration options and firewall rules that ensure compliance to security guidelines recommended by the following organizations:

- North American Electric Reliability Corporation (NERC): *Critical Infrastructure Protection (CIP) Reliability standards* CIP 001-009.[1]
- National Institute of Standards and Technology (NIST)**:** Special Publication 800-82, final public draft (September 2008). *Guide to Industrial Control Systems (ICS) Security*.
- National Institute of Standards and Technology (NIST)**:** Special Publication 800-53, Rev 2 (December 2007). *Information Security; Recommended Security Controls for Federal Information Systems*, Appendix I.
- Centre for Protection of National Infrastructure (CPNI): *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks* (February 2005).

Note: The security guidelines listed in this document stipulate that remote (off-site) users must be authenticated by the corporate firewall (see Figure 1 on page 10) before their connections are forwarded to the McAfee Firewall Enterprise for re-authentication and access authorization. For instructions, see the application note titled *Providing Secure Remote Access to Industrial Control Systems Using McAfee Firewall Enterprise (Sidewinder)*, available at mysupport.mcafee.com.

About industrial control systems

Industrial control systems (ICS) use commercial information technologies such as Ethernet, TCP/IP, and Windows for both critical and non-critical control and monitoring communications. Use of these commercial technologies results is significantly less isolation from the outside world for vital ICS systems in process control networks (PCNs).

About McAfee Firewall Enterprise

McAfee Firewall Enterprise employs SecureOS and Type Enforced Access Control as the backbone for strong security. SecureOS® is a hardened and enhanced UNIX operating system that employs patented Type Enforcement® security technology, resulting in superior network security and no emergency security patches to apply. To enforce network separation, McAfee Firewall Enterprise uses a logical division of network spaces called burbs. Burbs divide networks from each other, and each burb connects the firewall to systems with the same security requirements.

By reducing the administration footprint, enforcing separate domains for each process, and using a separate network stack for each network interface, SecureOS and Type Enforcement remove the inherent security risks often found in a network application running on non-security focused commercial operating systems.

1 This document was previously maintained by the NISCC (National Infrastructure Security Co-ordination Centre), which was incorporated into CPNI.

ICS security guidelines met by McAfee Firewall Enterprise

This section summarizes guidelines for Industrial Control System security, as extracted from the documents named in *About this document* on page 3. It also includes McAfee Firewall Enterprise configuration recommendations to address these guidelines. The guidelines are divided into the following sections:

Note: McAfee Firewall Enterprise allows only the traffic that matches the rules you have created. Many of the guidelines listed in the above sections should be addressed by adhering to best security practices when creating policy.

Network separation and segmentation

Table 1 shows network separation and segmentation security guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 1 Network separation and segmentation guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Use security zones (DMZs) to enforce network separation and prevent issues in one area from migrating to another. Group and separate key devices into zones with common security levels.	To enforce network separation: • Create a unique burb for each network you want to isolate. • If necessary, use VLANs to sub-divide LAN segments that are contained by burbs.
Use segmentation to restrict access: • Terminate all traffic in the DMZ. • Permit controlled communications between the DMZ and the corporate network and between the DMZ and the PCN. • Deny direct communications between the PCN and corporate network.	As necessary, create rules that allow selective communication between the following burb pairs: • DMZ and corporate • DMZ and PCN Do not create any rules that allow direct communication between the PCN and corporate burbs.
Place the Historian and similar plant information servers in a DMZ where they can communicate with PCN devices using insecure protocols such as MODBUS/TCP or DCOM and communicate with the corporate network using HTTPS, HTTP or SQL.	Create proxy rules to allow the Historian and plant information servers to communicate with: • PCN devices using SCADA protocols. • The corporate network using the HTTP, HTTPS, or SQL protocols.
Create an additional DMZ for controlling remote administration and service connections to the PCN.	Create a DMZ burb to contain remote administration and service connections.

Table 1 Network separation and segmentation guidelines *(continued)*

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Protect the PCN from the Internet: • Do not directly connect the PCN to the Internet, even if protected by a firewall. • Do not allow PCN devices to access the Internet directly or indirectly.	To ensure the PCN is not vulnerable to Internet threats: • Position your McAfee Firewall Enterprise (protecting the PCN) behind your corporate firewall. • Do not create rules that allow the PCN to reach the Internet.
Place the firewall at the perimeter of the PCN instead of inside the PCN to avoid blocking a critical alarm sent from a remote substation to your network's control center.	Deploy your McAfee Firewall Enterprise so that the entire PCN is self-contained inside the PCN burb.

Access control

Table 2 shows security guidelines for access control based on ports, protocols, addresses, and job function, and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 2 Access control guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Configure default firewall policy to disable all ports and services; deny all, permit none.	**No action required** – By default, McAfee Firewall Enterprise allows only administrative services.
Only allow the SCADA and industrial protocols, such as MODBUS/TCP, EtherNet/IP, and DNP317, within the process control network (PCN). Except for encrypted ICCP, do not allow these protocols to reach the corporate network.	**No action required** – McAfee Firewall Enterprise allows only the traffic that matches the rules you have created.
Isolate protocols that are allowed from the PCN to the DMZ: • Do not allow these protocols to reach corporate networks from the DMZ. • Do not allow these protocols to reach the DMZ from corporate networks.	When configuring your firewall to allow SCADA protocols to communicate between the PCN and DMZ, create rules that reference only the PCN and DMZ burbs.
Place the following restrictions on outbound traffic from the PCN to corporate networks: • Limit all outbound traffic from the PCN to the corporate network to essential traffic only. • Use firewall rules to allow only connections with a valid source address, destination IP address, service, and port.	When configuring your firewall to allow communication from the PCN to corporate networks, create rules that: • Allow only critical traffic to reach the corporate network. • Restrict access based on source, destination, protocol, and port.
Allow users to reach only the nodes on the PCN necessary for their job function.	Restrict access to the PCN by creating rules that: • Use authentication (for protocols that support it) to verify user identity. • Restrict access based on source IP address. • Restrict access based on destination IP address.
Provide a single or minimal connection that allows the PCN to be severed from the corporate network in times of serious cyber incidents.	**No action required** – The firewall PCN interface provides a single link between the PCN and your firewall. To sever the link, disable the interface or unplug the cable.

Common protocols

Table 3 shows protocol-specific security guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 3 Common protocol guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
DNS: • Use local DNS or a host file. • Do not allow DNS requests into the PCN. • Allow DNS requests from the PCN to DMZ on an individual basis by creating firewall rules.	Restrict DNS traffic as much as possible by creating DNS proxy rules that: • Only allow traffic from the PCN to the DMZ. • Use source and destination IP addresses to restrict access to the hosts that require it.
HTTP/HTTPS: • In general, do not allow HTTP from corporate networks to the PCN. • If required, allow access to specific PCN devices using either HTTPS or HTTP that is protected by a firewall proxy that blocks inbound scripts and Java applications.	If necessary, allow access to specific devices in the PCN from the corporate network by: • Creating HTTPS proxy rules. • Creating HTTP proxy rules using Application Defenses that are configured to block scripting and Java.
FTP/TFTP: • Block inbound FTP and TFTP. • If possible, use protocols that are more secure, such as Secure FTP (SFTP) or Secure Copy (SCP). • Allow outbound FTP only if it is secured with two-factor authentication and an encrypted tunnel.	Allow Secure FTP (SFTP) out of the PCN by creating SSH proxy rules that: • Use Application Defenses that are configured to allow SFTP. • Are configured to require user authentication. If you must allow FTP, configure a VPN to the destination FTP site to encrypt the FTP traffic.
Telnet: • Prohibit inbound Telnet sessions from corporate networks to the PCN unless secured with two-factor authentication and an encrypted tunnel. • Do not allow Telnet from the PCN to the DMZ or corporate network. • Allow outbound Telnet sessions only to specific devices over encrypted tunnels.	If possible, use SSH instead of Telnet. If Telnet is required: • Allow Telnet from the corporate network to reach the PCN by creating Telnet proxy rules that require user authentication. • For outbound Telnet connections, configure a VPN to the destination site to encrypt the Telnet traffic.
SMTP: • Do not allow inbound SMTP into the PCN. • Outbound SMTP from the PCN to the corporate network is acceptable for sending alert messages.	If you need to allow devices in the PCN to send alert messages to an SMTP server in the corporate network, create SMTP proxy rules that are restricted by source and destination IP address.
SNMP: • If possible, send only V3 commands. • Prohibit V1 and V2 commands unless sent over a separate, secured network.	If you need to allow SNMP traffic across insecure networks, configure a VPN to the destination site to encrypt the SNMP data.
RPC/DCOM: • Allow only between the PCN and DMZ. • Block between the DMZ and corporate networks. • Restrict the port ranges by making registry modifications on devices using RPC/DCOM.	Create packet filter rules to allow the required ports between the PCN and DMZ.

User authentication

Table 4 shows authentication security guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 4 User authentication guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Enforce secure authentication of all users seeking to gain access to the PCN.	Enable authentication on all rules that allow access to the PCN. Use the Passport authenticator if the protocol does not support conventional authentication.
Consider using separate authentication mechanisms, accounts, and credentials for access to the PCN and the corporate networks.	Configure your firewall to perform authentication in conjunction with different external authentication servers.
Lock out accounts with excessive login attempts.	Use the McAfee Firewall Enterprise Authentication Failure Lockout feature to lock out users who fail authentication after a configured number of attempts.
Store passwords using non-reversible encryption.	**No action required** – McAfee Firewall Enterprise user and administrator passwords are stored using non-reversible encryption.
Eliminate duplicate or shared passwords and immediately delete vendor-supplied passwords.	Use an external authentication sever to mitigate password management issues.

Network address translation (NAT)

NAT involves rewriting the source address of a packet to a new IP address specified by the administrator. Reasons to use NAT include:

- Hiding your internal network addresses from public view.
- Replacing private addressing on outbound traffic with publicly routable address.

Table 5 shows NAT deployment guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 5 NAT guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Do not deploy NAT between the PCN and DMZ because of its impact on protocols such as EtherNet/IP, Foundation Fieldbus, and OPC.	Do not enable NAT on rules that allow access between the PCN and the DMZ.
If desired, deploy NAT between the DMZ and the corporate network.	As necessary, enable NAT on rules that allow access between the DMZ and the corporate network.

Remote access

Table 6 shows remote access security guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 6 Remote access guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Require authentication and use encrypted protocols such as VPN or HTTPS for Internet or dial-up remote access connections.	To secure remote access connections: • Create VPNs for remote access connections. • Create HTTPS proxy rules with SSL decryption enabled that require authentication.
Once connected to the corporate network, require users to re-authenticate a second time with a personal and unique password using a strong two-factor authentication method to access the PCN.	To require strong authentication: • For VPNs, enable extended authentication using a strong authentication method, such as Aladdin SafeWord. • For HTTPS proxy rules with SSL decryption, enable a strong authentication method.
For organizations that do not permit unencrypted control traffic to traverse the corporate network, require a secondary tunneling solution, such as an IPsec tunnel between the remote access point and a PCN or DMZ.	Create a VPN between your McAfee Firewall Enterprise and your corporate firewall to encrypt control traffic that passes over the corporate network.

Virus scan and intrusion detection/prevention management

Table 7 shows virus scan and intrusion detection/prevention management guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

Table 7 Virus scan and intrusion detection/prevention guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
Deploy intrusion detection software.	Enable McAfee Firewall Enterprise Signature-based Intrusion Protection Service (IPS) on proxy rules that protect critical devices. McAfee Firewall Enterprise IPS supports over 10,000 signatures that represent known network-based intrusion attacks, including 28 signatures for three SCADA protocols: MODBUS/TCP, DNP3/TCP, and ICCP/TCP.
Deploy antivirus software.	Enable the McAfee Firewall Enterprise anti-virus module on HTTP, FTP, and Sendmail rules to detect and block viruses, spyware, and prohibited MIME extensions.
Before deploying IDS/IPS software, perform extensive testing to determine that it does not compromise normal operation of the industrial control system (ICS).	Enable an IPS signature group on an active rule while specifying an Allow response mapping. This allows you to test IPS in an active environment to determine if it will interfere with normal operation of the ICS. If not, enable a response mapping to take action against positive matches.

Firewall management, logs, and audit

Table 8 shows virus scan and intrusion detection/prevention management guidelines and the McAfee Firewall Enterprise configuration necessary to satisfy each guideline.

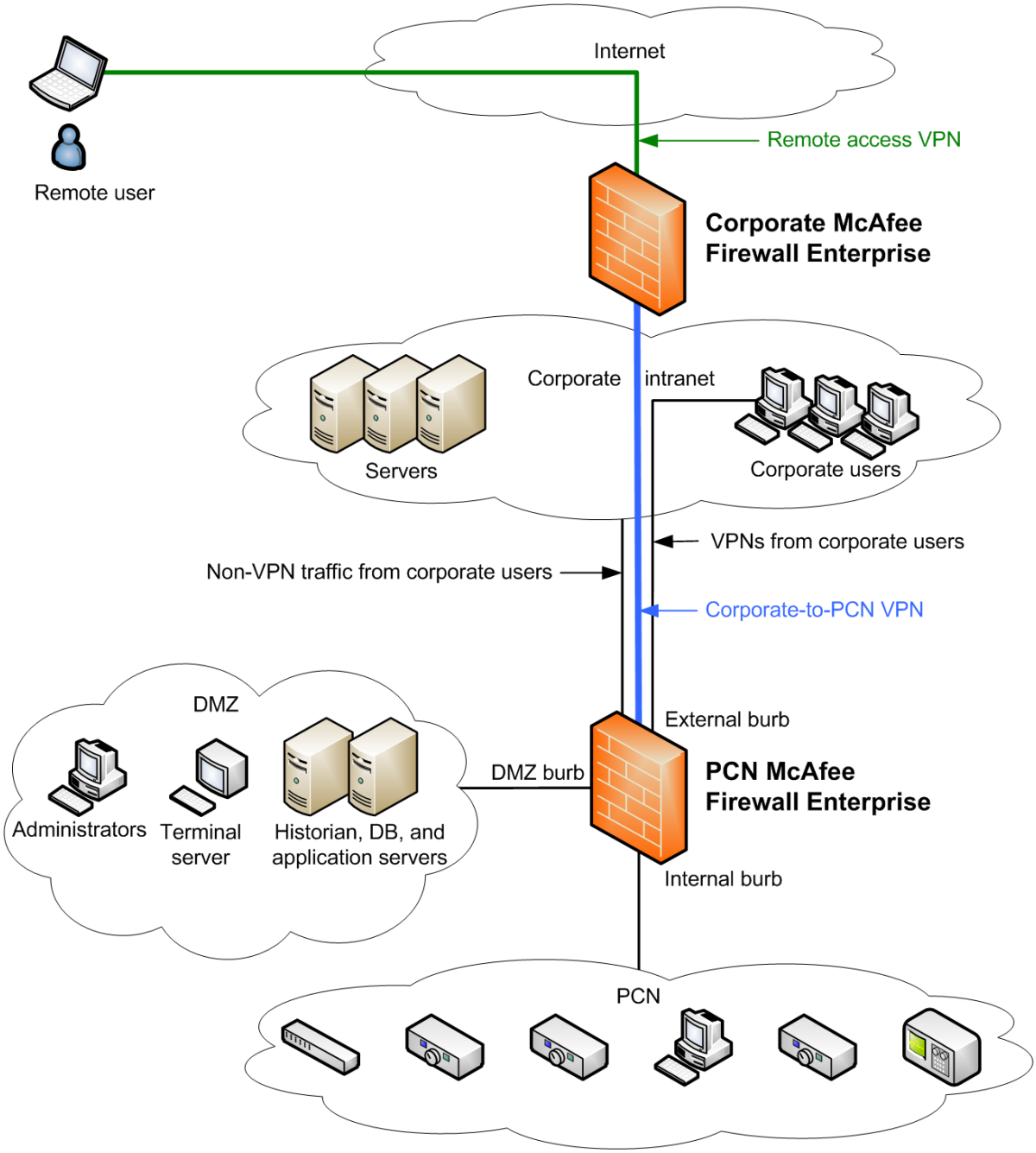
Table 8 Firewall management, logs, and audit guidelines

Security guidelines	McAfee Firewall Enterprise configuration recommendation
All firewall management traffic must be: • Initiated from a management station that is configured with a static IP address. • Contained on a separate out-of-band, secured management network or over an encrypted network with two-factor authentication.	Configure the Admin Console rule to use a strong authentication method. Note: McAfee recommends configuring a secondary authentication method to avoid losing administrative access to your firewall in the event of an authentication server failure.
To keep syslog data secure: • Restrict access to syslog data to authorized users. • Use VPNs to secure the data outside the PCN and DMZ networks.	Configure your firewall to send syslog data to a syslog server in the DMZ. If the syslog server is located on an insecure network, create a VPN to the syslog server site to encrypt the audit data.
Record information flow for traffic monitoring, analysis, and intrusion detection.	Retain firewall audit data by performing one of the following actions: • Configure Audit Management to regularly export the firewall audit data to an external server. • Use syslog data sent to a syslog sever to retain audit information.
Ensure that each critical component has a redundant counterpart. If a component fails, it should fail in a manner that does not generate unnecessary traffic or cause another problem elsewhere.	Deploy two firewalls in a High Availability configuration for redundancy.

Deployment scenario

The deployment scenario shown in Figure 1 depicts an example network configuration that satisfies the requirements in *ICS security guidelines met by McAfee Firewall Enterprise* on page 4. In this example configuration, a McAfee Firewall Enterprise protects the process control network from the corporate network and isolates systems that need to interact with the PCN in a DMZ.

Figure 1 Deployment scenario



Use of burbs in this scenario

A burb is used to isolate network interfaces from each other. In this deployment scenario, the McAfee Firewall Enterprise is configured with five burbs:

- **External** – An external interface and burb connected to the corporate intranet via a network interface card (NIC)
- **Internal** – An internal interface and burb connected to the PCN via a NIC
- **DMZ** – An interface and burb connected to the DMZ via a NIC

  The DMZ hosts the Historian, terminal, web, application, and authentication servers. It also hosts non-time critical resources associated with backup/recovery, network monitoring and management, printing, document control, and other hosts that require restricted PCN access.
- **Virtual-1** – A virtual burb (not physically connected to a NIC) for terminating remote access VPNs arriving from the Internet, dial-up, or WANs via the corporate firewall
- **Virtual-2** – A virtual burb (not physically connected to a NIC) for terminating VPNs from users on the corporate intranet

Scenario assumptions and caveats

- Network address translation (NAT):
  - On McAfee Firewall Enterprise, network address translation (NAT) is configured on a per-rule basis. In this deployment scenario, it is assumed that the IP addresses on the PCN are routable within the corporate network. Therefore, NAT is unnecessary for users accessing the PCN from the corporate intranet.
  - For IPsec VPN connections from off-site remote users, NAT is optional because IPsec VPNs encapsulate the endpoint addresses inside the encrypted tunnels, making them invisible on the Internet. However, you can use NAT to hide the PCN addresses from the remote user.
- Virtual private networks (VPNs):
  - In this scenario, the McAfee Firewall Enterprise has no direct connection with the Internet, dial-up connections, or WANs. Therefore, any connections from these sources must first traverse the corporate firewall and intranet. To access the DMZ, remote users must authenticate at the corporate firewall and then re-authenticate at the McAfee Firewall Enterprise guarding the PCN using PCN credentials. This scenario assumes that your organization does not permit unencrypted PCN control traffic to traverse the corporate network for security reasons. To meet this requirement, a separate gateway-to-gateway IPsec tunnel is required to forward the packets to the McAfee Firewall Enterprise from the corporate firewall.
  - Access from dial-up connections or WANs may use existing methods which should include first logging into the corporate firewall. Similar to VPN connections from remote users, the corporate firewall forwards the packets to the McAfee Firewall Enterprise inside the gateway-to-gateway IPsec tunnel. The McAfee Firewall Enterprise will re-authenticate the user, then scan and filter the packets entering the DMZ.
- Authentication:
  - The security guidelines stipulate that remote users should be authenticated by the corporate firewall before their connections are forwarded to the McAfee Firewall Enterprise for re-authentication and access authorization. A separate application note provides instructions for configuring both the corporate firewall and the McAfee Firewall Enterprise to support this cooperative access method.
  - The configuration in Figure 1 on page 10 does not show an authentication server capable of providing strong two-factor authentication, which the security guidelines strongly recommend. McAfee recommends that you deploy an authentication server such as RSA SecureID or Aladdin SafeWord in the DMZ.

Create your security policy

This section contains a roadmap for configuring McAfee Firewall Enterprise to satisfy your organization's security policy. Use the steps outlined below to configure your McAfee Firewall Enterprise.

Plan your security policy

To plan your security policy, compare the requirements of your network to the rules listed in the table below. The table contains a minimum set of rules that are valid for the configuration scenario shown in Figure 1 on page 10. Make any necessary additions or changes as required by your network.

Note: Because TCP/IP networks are not deterministic, take steps to ensure that time-critical events are not transmitted over the TCP networks.

Table 9 Example rules

Purpose	Service	Source Burb	Destination Burb
Monitoring and control	Modbus/TCP proxy	Internal	DMZ
	Modbus/TCP proxy	DMZ	Internal
	DNP3/TCP proxy	Internal	DMZ
	DNP3/TCP proxy	DMZ	Internal
	ICCP/TCP proxy	Internal	DMZ
	ICCP/TCP proxy	DMZ	Internal
	DCOM proxy	Internal	DMZ
	DCOM proxy	DMZ	Internal
	EtherNet/IP proxy	Internal	DMZ
	EtherNet/IP proxy	DMZ	Internal
Alert messages	SMTP/UDP proxy	PCN	External
Remote administration and maintenance	Telnet proxy	Virtual-2	DMZ
	Remote desktop proxy	Virtual-2	DMZ
Access to data historian	HTTPS proxy	External	DMZ
	HTTPS proxy	Virtual-1	DMZ
	HTTPS proxy	Virtual-2	DMZ

Perform the initial configuration procedure

Perform the initial configuration procedure as documented in the *McAfee Firewall Enterprise Setup Guide*, available at mysupport.mcafee.com. These steps include:

- Installing the McAfee Firewall Enterprise Management Tools on a Windows-based computer.
- Running the Quick Start Wizard.
- Connecting to the firewall using the Admin Console.

When initial configuration is complete, continue with *Configure networking* on page 13.

Configure networking

To configure your McAfee Firewall Enterprise to connect to the appropriate networks, perform the following procedures:

- *Configure burbs* on page 13
- *Configure network interfaces* on page 14

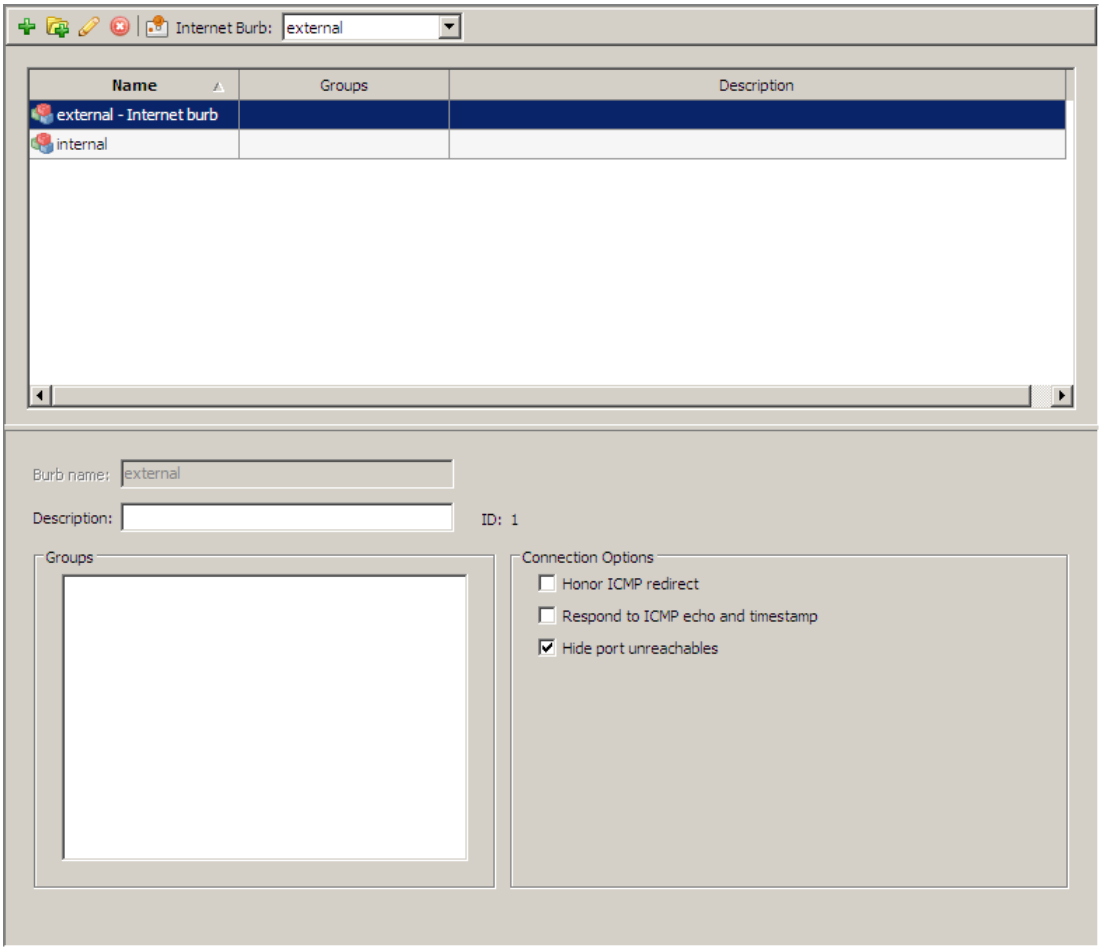
Configure burbs

A burb is used to isolate network interfaces from each other.

- An internal burb and an external burb are defined on your firewall during the installation process.
- You create, modify, and delete burbs in the Burb Configuration window.
- You select these burbs as Source and Destination burbs when creating a rule in the Rules window.

To create burbs: select **Network > Burb Configuration**.

Figure 2 Burb Configuration window



The upper pane lists existing burbs. The external and internal burbs are pre-configured by default.

For more detailed information, see the "Burbs, Interfaces, and Quality of Service" chapter of the *McAfee Firewall Enterprise Administration Guide*.

Configure network interfaces

An interface is a boundary that two systems communicate across.

- You assign all the network link elements to the interface, such as IP address, network mask, burb, NIC, and MTU size for outgoing packets.

  Note: The Network Interface Card (NIC) is the hardware device that the network cable is plugged into.

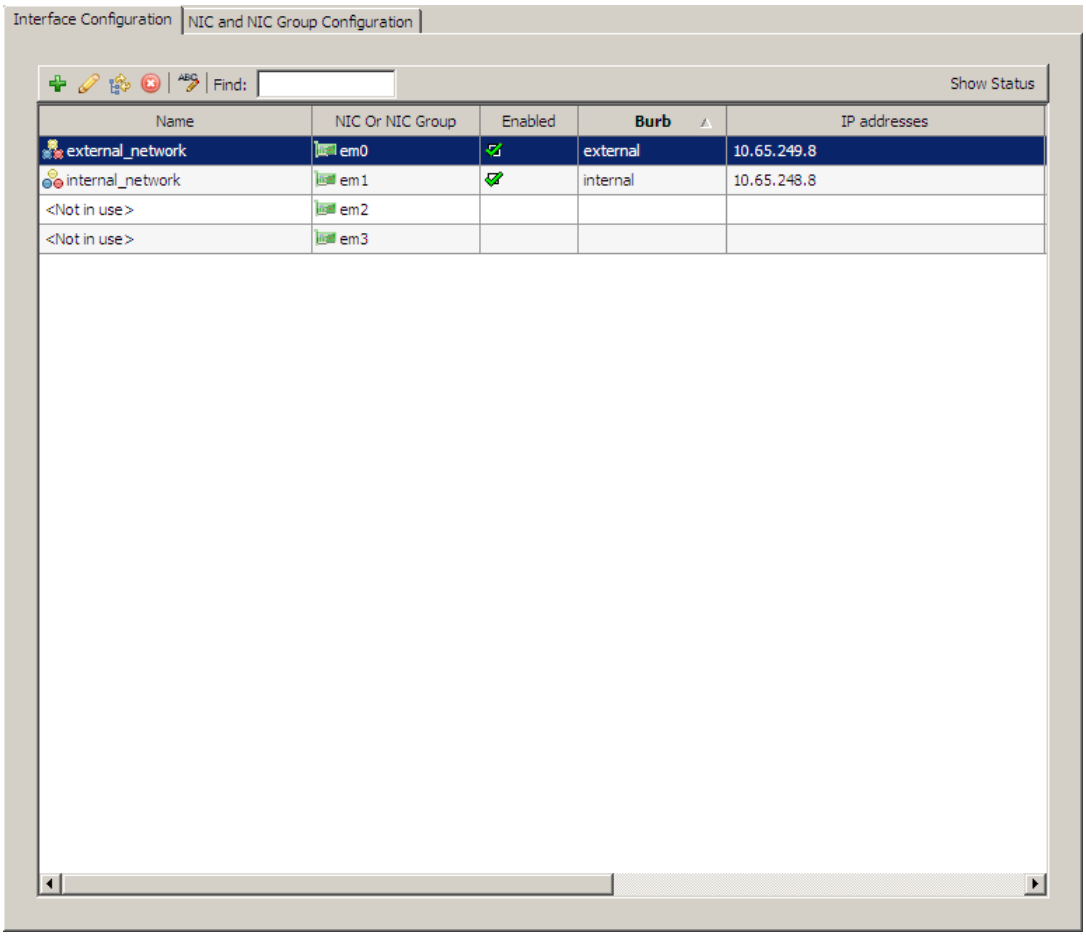
- You can create Standard, VLAN, DHCP, or transparent interfaces.
- An interface can have IPv4 addresses, IPv6 addresses, or both.

  Note: Transparent interfaces do not support IPv6.

- You can select Quality of Service Profiles and define alias addresses for an interface.
- By using VLANs, you can create up to:
  - 512 interfaces on a standalone firewall.
  - 255 interfaces on a High Availability cluster.
- The internal and external network interfaces of the firewall are defined during the initial configuration.

Use the Interfaces window to configure network interfaces: select **Network > Interfaces**.

Figure 3 Interfaces window



For detailed instructions, see the "Burbs, Interfaces, and Quality of Service" chapter of the *McAfee Firewall Enterprise Administration Guide*.

Configure rule elements

Rule elements are the building blocks of rules. To create rules, first configure the elements that the rules will reference:

- *Configure Network Objects* on page 15
- *Configure authentication* on page 15
- *Configure services* on page 17

Note: You can also create Application Defenses to configure advanced properties for rules. To manage Application Defenses, select **Policy > Rule Elements > Application Defenses > Defenses**.

Configure Network Objects

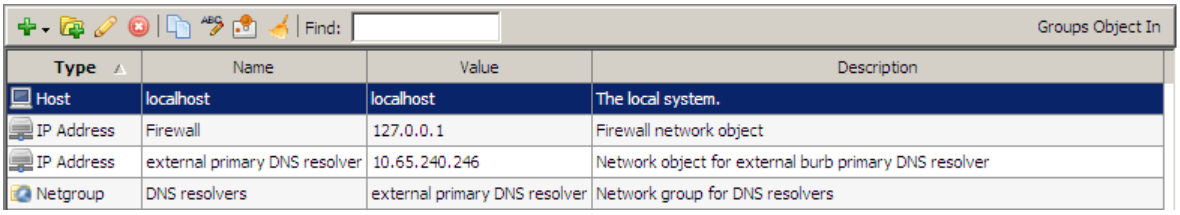
A network object is the source or destination of a connection to or through the McAfee Firewall Enterprise. A network object can be any of the following:

- Domain
- Geo-Location
- Host
- IP address
- IP range
- Netmap
- Subnet
- Netgroup

Each network object that you create is available for selection from the source and destination Endpoint drop-down lists on the Rules window.

Use the Network Objects window to configure network objects: select **Policy > Rule Elements > Network Objects**.

Figure 4 Network Objects window



For detailed instructions, see the "Network Objects and Time Periods" chapter of the *McAfee Firewall Enterprise Administration Guide*.

Configure authentication

Authenticators validate a person's identity before he or she is allowed to pass traffic through the firewall.

McAfee Firewall Enterprise supports the following authentication methods:

- **Passport** – Passport (also known as single sign-on) associates an authenticated user with their IP address. A successful Passport authentication caches the source IP address for a specified time. Subsequent connection attempts from the same IP address are allowed without prompting for authentication.

  Security level: Weak

- **Password** – Standard password authentication requires a user to enter the same password each time he or she logs in.

  Security level: Weak

- **LDAP (Lightweight Directory Access Protocol)** – Four types of LDAP authentication are available: iPlanet, Active Directory, OpenLDAP, and Custom LDAP.

  Security level: Weak

- **Windows Domain** – You can use this authenticator if your organization operates a Windows primary domain controller (PDC) or backup domain controller (BDC).

  Security level: Weak

- **RADIUS** – You can use this authenticator if your organization operates a RADIUS server.

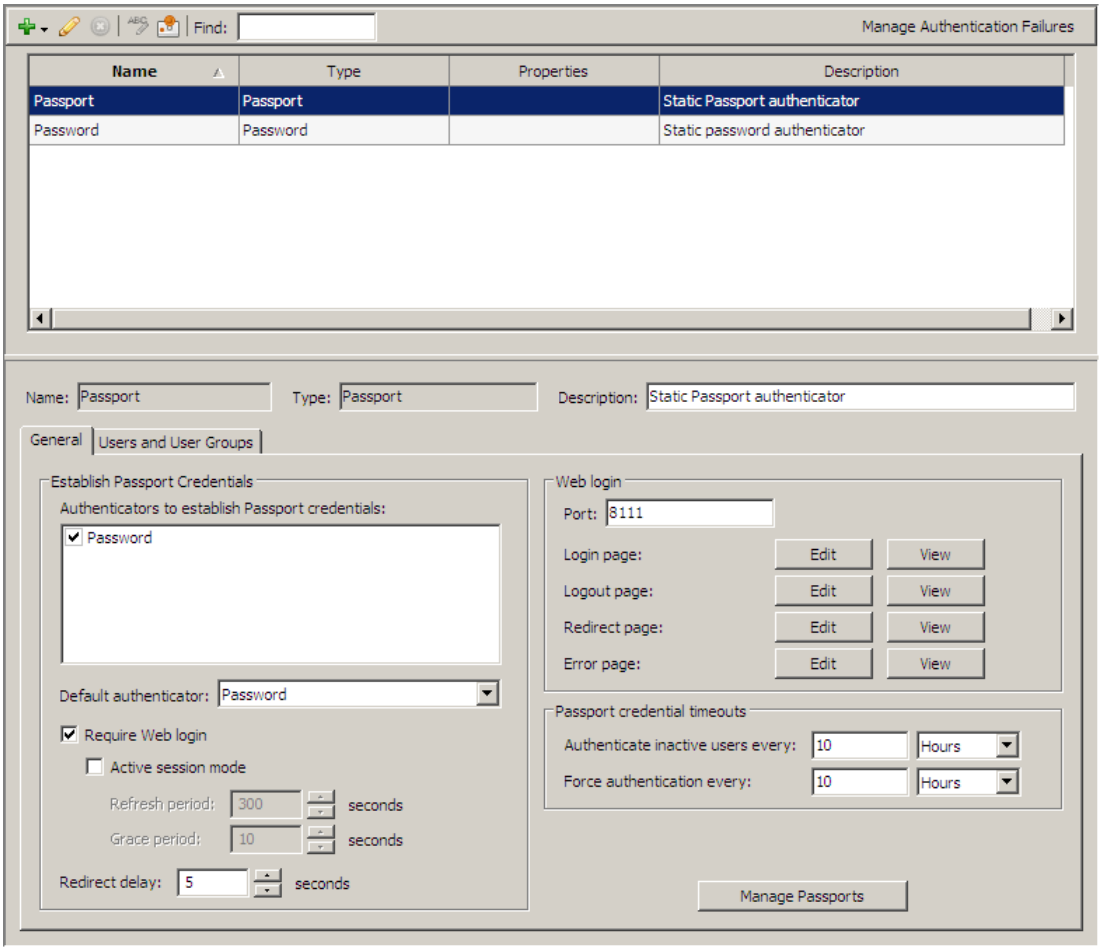
  Security level: Varies with authentication server and method

- **SafeWord** – SafeWord RemoteAccess and SafeWord PremierAccess interoperate with McAfee Firewall Enterprise.

  Security level: Varies with authentication server and method

Use the Authenticators window to configure authenticators: select **Policy > Rule Elements > Authenticators**.

Figure 5 Authenticators window



For detailed instructions, see the "Authentication" chapter of the *McAfee Firewall Enterprise Administration Guide*.

Configure services

A McAfee Firewall Enterprise service associates a traffic's transport layer with a specific agent that is responsible for managing the service's traffic. The transport layer information includes elements such as the protocol, the ports, and the idle timeout. A rule use a service, along with source and destination information, to determine what traffic that rule will allow or deny. You create a service by selecting an agent, assigning it specific transport-layer properties, giving it a name, and then saving it.

An agent is responsible for handling traffic and can be one of these types:

- Proxy
- Filter
- Server

The firewall provides predefined TCP-based proxy services for a variety of Internet services including HTTP, Telnet, FTP, and many others. The firewall also supports proxy services for routing UDP transmissions for applications based on protocols such as SNMP and NTP.

Table 10 contains a non-comprehensive list of services that you may need to create to allow SCADA protocols through your McAfee Firewall Enterprise.

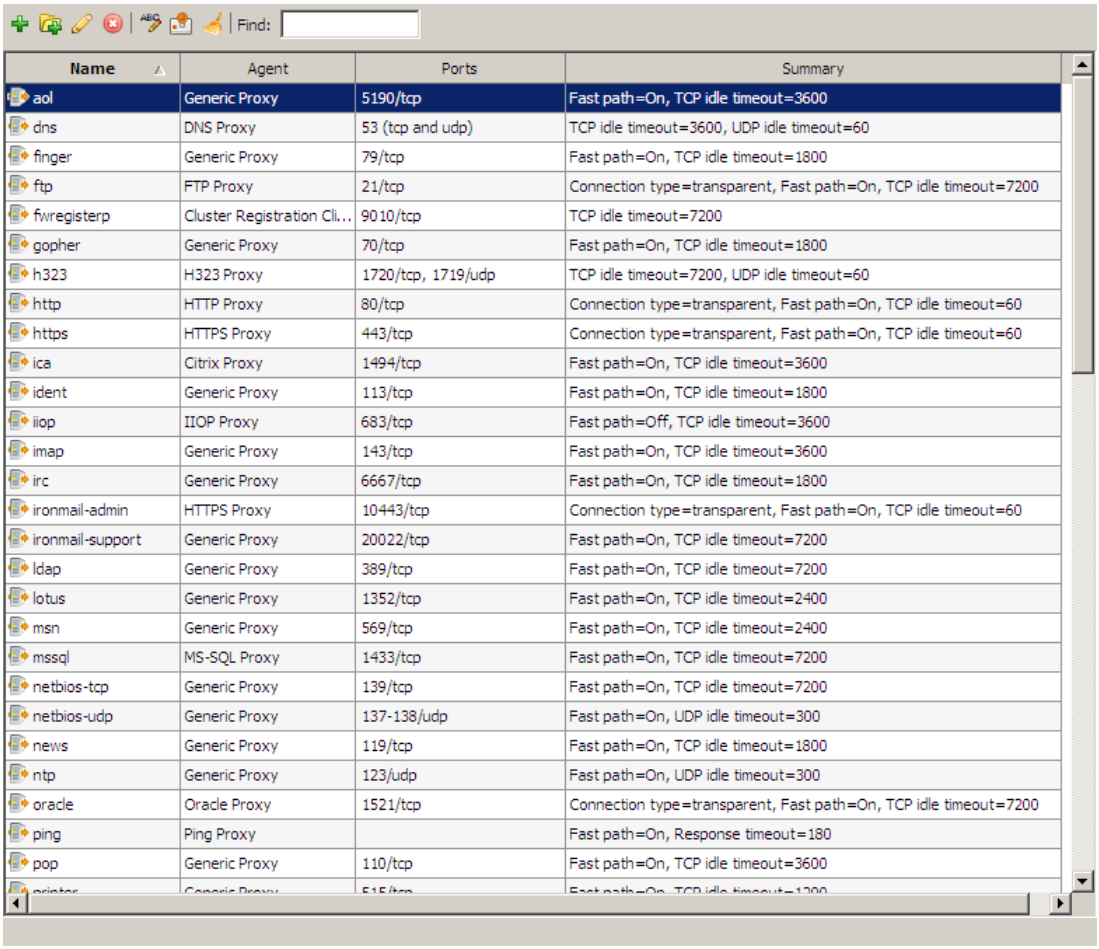
Note: The ports shown in Table 10 represent well known or registered ports. Before creating services for these protocols, investigate to determine what ports are in use on your network.

Table 10 Services that you may need to create

Protocol	Port	Recommended service type
Remote desktop	TCP 3389	Generic Proxy
SMTP/UDP	UDP 161	Generic Proxy
Modbus/TCP	TCP 502	Generic Proxy
DNP3/TCP	TCP 20000 UDP 20000	Generic Proxy
ICCP/TCP	TCP 102	Generic Proxy
DCOM	TCP 135 (Windows 95 or later) UDP 135 (Windows NT 4.0)	Generic Proxy
EtherNet/IP	TCP/UDP 44818 TCP/UDP 2222	Generic Proxy

Use the Services window to configure services: select **Policy > Rule Elements > Services**.

Figure 6 Services window



For detailed instructions, see the "Services" chapter of the *McAfee Firewall Enterprise Administration Guide*.

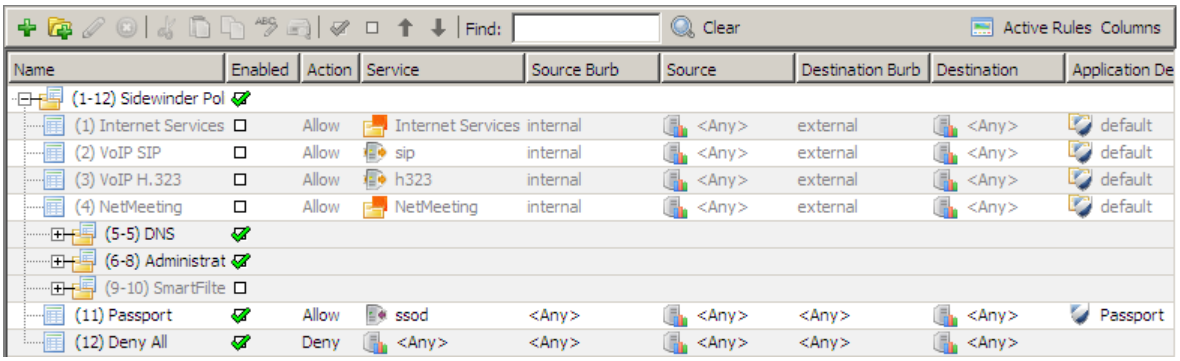
Create rules

Rules are the basis of your security policy. They determine what traffic will be allowed to pass through your McAfee Firewall Enterprise and what will be denied.

About the Rules window

Use the Rules window to manage rules: select **Policy > Rules**.

Figure 7 Rules window



This window provides an overview of your security policy. It is where you view rules, adjust rule order, and enable or disable rules. It is also the starting point for creating and modifying rules and rule groups.

The order in which rules and nested groups of rules appear is significant. When the firewall is looking for a rule match, it searches the enabled rules sequentially beginning with the first rule or nested group within the group, then the second, and so on. If the traffic does not match the first rule, it is forwarded on to the next rule. Once a rule match is found, the traffic is processed according to that rule and the search stops. You should always place rules that allow or deny the most frequent traffic near the top of your security policy to reduce processing time.

The default policy contains a Deny All rule at the end of the policy. This rule denies any traffic that reaches it. The rule itself is a reminder that any traffic that does not match a rule is automatically denied; even if the Deny All rule is deleted, the firewall denies any traffic that does not find an exact match in your security policy. By default all services and ports are disabled until enabled by "permit" rules. After installation, McAfee Firewall Enterprise remains in a deny all/permit none state until permit rules are configured and applied. Ensure that Deny All is at the bottom of the list.

Example of a simple rule

This section provides an example of a simple rule to help you better understand how the firewall uses a rule to determine whether to allow or deny a connection request, and how to handle allowed connections.

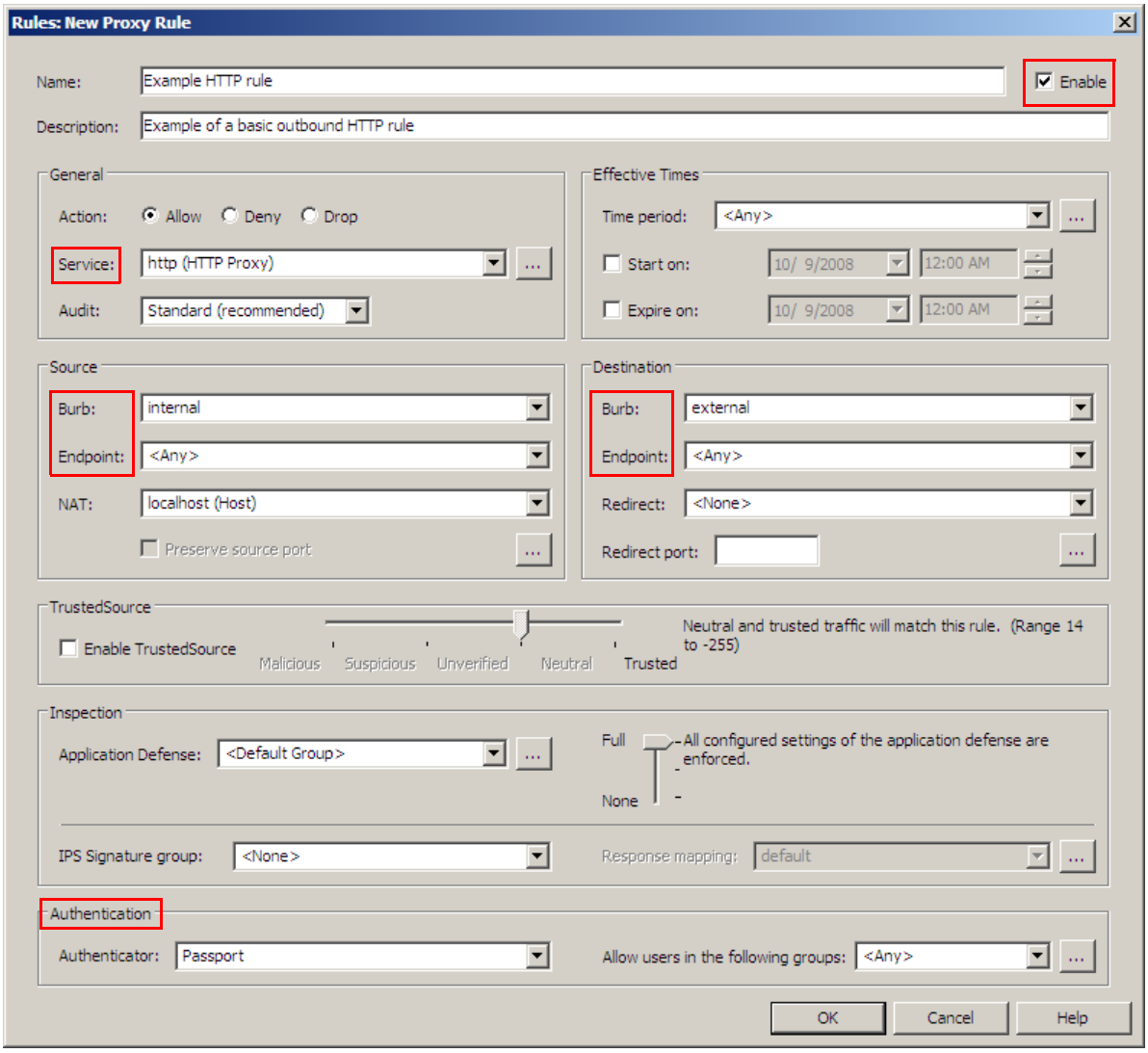
Table 11 lists the condition elements for a rule that permits any client in an internal burb to connect to any Web server located in the external burb. Conditional elements are the elements that a rule examines to see if a packet matches that rule. The fields corresponding to the criteria described in the table are indicated in Figure 8.

There are also a number of action elements you can configure for each rule. After a rule determines that a packet matches its condition elements, the rule handles the packet according to the action elements' values. The action elements are: whether or not to allow the connection or session, what amount of audit data to generate, if the address should be translated, what Application Defense settings to enforce, and if the traffic will be compared to a set of IPS signatures.

Table 11 Rule elements that determine if a packet will match a rule

Condition rule elements	Setting	Comments
Enable	Checked	Disabled rules do not process traffic.
Service	HTTP (HTTP Proxy)	This rule uses the default HTTP proxy service, which accepts HTTP traffic on TCP port 80 and passes traffic transparently (browsers do not need to point to the firewall).
Source Burb	internal	Traffic will originate in the internal burb.
Source Endpoint	<Any>	Traffic can originate from any IP address in the internal burb.
Destination Burb	external	Traffic will be delivered to the external burb.
Destination Endpoint	<Any>	Traffic can be delivered to any IP address reachable via the external burb.
Authentication	Passport	Users must authenticate the first time they use this rule to connect to an external Web server. Subsequent connections will be authenticated from a cache.

Figure 8 A basic rule with condition elements



Create a rule

Use the New Rule window to create rules: from the Rules window click **New Rule**.

Specify a name, and then configure the following elements:

- **Service**
- **Source Burb**
- **Source Endpoint**
- **Destination Burb**
- **Destination Endpoint**
- **Authentication** (optional)

Tip: The other configurable rule elements are optional and offer additional functionality. Leave these elements at the default values unless you need this additional functionality.

For detailed instructions, see the "Rules" chapter of the *McAfee Firewall Enterprise Administration Guide*.

Create a VPN to allow corporate users to access the PCN

This section creates an example VPN to provide PCN access to users on the corporate network. Its main purpose is to hide the traffic inside an encrypted tunnel as it traverses the corporate network. This VPN has the following attributes:

- Computer identification by shared secret (also referred to as password).

  Tip: For large deployments McAfee recommends using either McAfee Firewall Enterprise self-signed or Certificate Authority-issued client certificates.

- User authentication via the extended authentication (XAUTH) method. While this example configuration uses fixed passwords stored by McAfee Firewall Enterprise, a two-factor authentication method is strongly recommended.
- VPN termination in a virtual burb named Virtual-2.

Note: For this example, it is assumed that NAT is enabled on the corporate firewall.

To configure the example VPN:

- *Enable extended authentication on the ISAKMP server* on page 21
- *Allow access to the ISAKMP server* on page 22
- *Create a client address pool* on page 22
- *Create the VPN definition* on page 23

For detailed instructions, see the "Virtual Private Networks" chapter of the *McAfee Firewall Enterprise Administration Guide*.

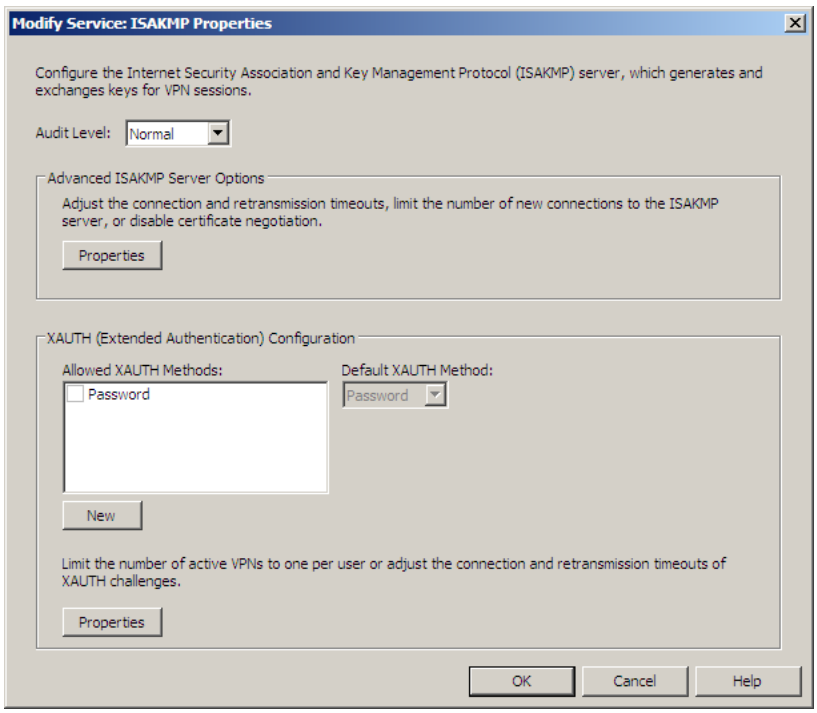
Enable extended authentication on the ISAKMP server

The ISAKMP server is used to generate and exchange keys for VPN sessions and includes properties for audit, negotiating connections, and extended authentication parameters.

To enable extended authentication:

1. Select **Policy > Rule Elements > Services**.
2. Select **isakmp** and then click **Modify**.

Figure 9 ISAKMP Properties window



3 In the **Allowed XAUTH Methods** field, select **Password**.

4 Click **OK** and save your changes.

Allow access to the ISAKMP server

Create a rule to allow access to the ISAKMP server:

1 Select **Policy > Rules**.

2 Click **New** to create a rule for the ISAKMP service. The rule must contain the following values:

- **Service** – isakmp (ISAKMP Server)
- **Source Burb** – external
- **Source Endpoint** – A netgroup network object containing the IP addresses on the corporate network that can initiate VPN connections
- **Destination Burb** – external

3 Save your changes.

Create a client address pool

To create a client address pool:

1 Select **Network > VPN Configuration > Client Address Pools**.

2 Click **New** and specify the following:

- **Pool Name** – Specify a name, such as *Corporate_Users_Pool*.
- **Virtual Subnet** – Type a subnet out of which the firewall will assign addresses to VPN clients.
- **Define the Local Subnets available to remote clients** – Add the network(s) in the PCN that VPN users will be allowed to access.

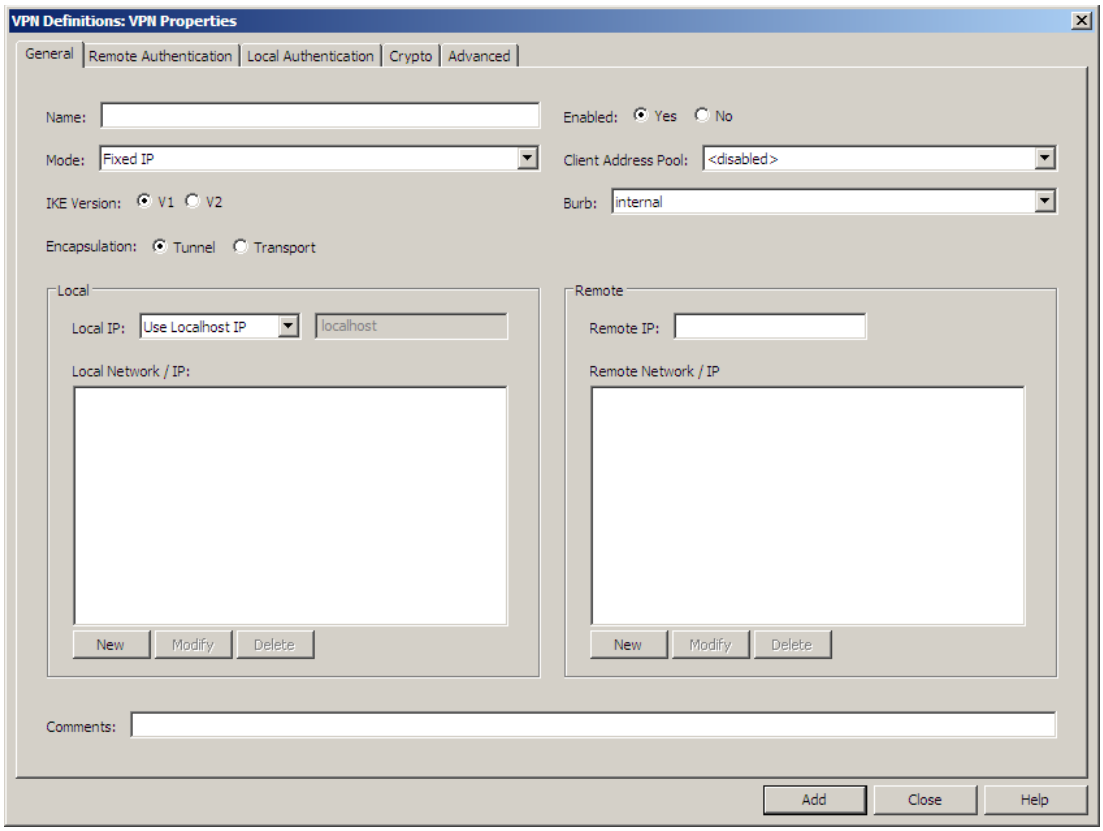
3 Click **Add** and then save your changes.

Create the VPN definition

To create a VPN definition:

1 Select **Network > VPN Configuration > VPN Definitions**, and then click **New**.

Figure 10 VPN General tab



2 On the **General** tab, specify the following:

- **Name** – Corporate_Users
- **Mode** – Dynamic IP Restricted Client
- **IKE version** – V1
- **Encapsulation** – Tunnel
- **Enabled** – Yes
- **Client Address Pool** – Corporate_Users_Pool
- **Burb** – Virtual-2
- **Local IP** – Use Localhost IP

3 On the **Remote Authentication** tab, specify the following:

- **Remote Authentication Method** – XAUTH + Password
- **Enter Remote Password** – Type a password.
- **Verify Remote Password** – Confirm the password.
- **Remote Identity** – Click **Remote Identities** and create a remote identity that will be shared among corporate VPN users.

4 On the **Local Authentication** tab, specify the following:

- **Local Identity Type** – IP Address
- **Value** – localhost

5 On the **Advanced** tab, change the **IKE V1 Exchange Type** to Aggressive.

6 Click **Add**. A Confirm window appears.

7 Click **Yes** and then save your changes.

Perform post-configuration tasks

After you have created rules to implement your security policy, perform the following tasks:

- *Test your configuration* on page 24
- *Enable command line access* on page 24
- *Create an alternate policy* on page 24
- *Create a configuration backup* on page 24

Test your configuration

Confirm that the required traffic is passing between the PCN, DMZ, and corporate networks. Use the Audit Viewing window to obtain troubleshooting information: select **Monitor > Audit Viewing**.

Enable command line access

For troubleshooting purposes, enable Secure Shell (SSH) command line access.

1 Select **Policy > Rules**.

2 In the Administration rule group, enable the **Secure Shell** rule.

3 Modify the rule's endpoints and authentication as needed.

4 Use an SSH client to confirm that you can connect to your firewall.

Create an alternate policy

Create a policy that enables quick disconnect from the corporate network in case of attack.

1 In the Policy window, create a rule group for the alternate policy.

2 In that group, place all the rules needed to implement the alternate policy. Be sure to create a Deny All rule as the last rule of the alternate policy rule group.

Tip: Rule groups can be nested within other groups.

3 When you have finished creating the alternate policy, disable the policy by selecting the alternate policy rule group and clicking **Disable**.

4 To use the alternate policy, move the alternate policy rule group to the top of the rule list and enable it. The firewall begins enforcing your alternate policy.

Create a configuration backup

Use the Configuration Backup window to create a backup of your firewall's configuration: select **Maintenance > Configuration Backup**.

Tip: Save the configuration backup to your client system or a remote system to avoid losing it due to hardware failure.

Glossary

A

Admin Console	The graphical user interface (GUI) used to configure and manage McAfee Firewall Enterprise. The Admin Console runs on Windows-based platforms.

B

burb	McAfee Firewall Enterprise uses a logical division of network spaces called burbs. Burbs divide networks from each other, and each burb connects the firewall to systems with the same security requirements.

D

DMZ (demilitarized zone)	A network buffer zone that often hosts services that require interaction the Internet, while still protecting internal systems. On McAfee Firewall Enterprise, the DMZ is generally a burb for hosting web servers and other hosts that receiving large volumes of external, untrusted traffic.

E

extended authentication (XAUTH)	An extension of the IKE protocol that allows the administrator enforce user-based authentication in addition to the existing IKE authentication. It initiates after the existing IKE authentication mechanism is successful. XAUTH associates the VPN session to the user who authenticated, and enables use of strong authentication in VPN configurations.

F

FTP (file transfer protocol)	A protocol used on the Internet for transferring files.

H

HTTP (hypertext transfer protocol)	A protocol that requests and transfers HTML documents on the World Wide Web.
HTTPS (hypertext transfer protocol secure)	An agreed-upon format (protocol) that requests and transfers HTML documents on the World Wide Web in a secured manner.

I

ICS (industrial control system)	A term for control systems used in the industrial and critical infrastructure sectors, including supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS).
IKE (Internet key exchange)	A key management protocol standard which automates the implementations of other protocols (ISAKMP, Oakley, etc.) used in a VPN connection.
IP address	For IPv4, a 32-bit address that uses standard dotted quad notation assigned to TCP/IP network devices. An IP address is unique to each machine on the Internet. An IP address contains a network and host field. For IPv6, the address is 128 bits and is normally written as eight groups of four hexadecimal digits.
IPS (Intrusion Prevention System)	A system for identifying attacks before they pass through the firewall. McAfee Firewall Enterprise has a signature-based IPS feature that is configurable on packet filter, proxy, and server rules, and has an IPS Attack Response feature that sends alerts based on audit events.
IPsec (Internet Protocol Security)	A set of standards created to provide data integrity and confidentiality at the IP layer of the network stack.

ISAKMP (internet security association and key management protocol) A protocol framework which sets the parameters for a VPN connection by defining the payload format, how the key exchange protocol will be implemented, and how the security association will be negotiated.

N

NAT (network address translation) Rewriting the source address of a packet to a new IP address specified by the administrator. The term NAT is often applied when the firewall rewrites the source address. See redirection for when the firewall rewrites the destination address.

NIC (network interface card) Hardware, like a computer circuit board, that contains a port or a jack that enables a computer to connect to network wiring, such as an ethernet cable, a phone line, etc.

P

packet filter A service that provides the ability to specify rules for IP-based traffic to flow through the firewall at the network layer or the transport layer of the network stack.

Passport A login process that requires a user to enter the same password each time he or she logs in. This method is the most common form of authentication security.

PCN (process control network) A network that allows communication between control and measurement units and Supervisory Control and Data Acquisition (SCADA) equipment.

port The number that identifies the destination application process for transmitted data. Port numbers range from 1 to 65535. For example, Telnet typically uses port 23, DNS uses 53, etc.

proxy A software agent that acts on behalf of a user requesting a network connection through the firewall. The proxy agent accepts a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, optionally does additional authentication, and then completes a connection on behalf of the user to a remote destination.

R

rule A rule is a mini policy which contains criteria that is used to inspect incoming or outgoing traffic. Rules determine whether that traffic will be allowed to continue to its destination. Rules are created for three types of firewall services: packet filter, proxy, or server.

rule group An organized set of rules. A rule group can consist of both rules and nested rule groups.

S

SCADA A supervisory control and data acquisition system that monitors and controls a process.

SecureOS™ The UNIX-based operating system used in a McAfee Firewall Enterprise system. SecureOS is built upon FreeBSD and includes Type Enforcement security mechanisms.

service A firewall service is a server, proxy, or packet filter that provides the control for a specific internet service, such as HTTP, FTP, or Telnet. It consists of an agent, transport-layer properties, and, depending on the agent, agent-specific properties.

server A computer system that provides services (such as FTP) to a network, or a program running on a host that offers a service to other hosts on a network.

strong authentication A login process that requires a user to enter a unique, one-time response to a login challenge or special code presented by an authentication server. The user must make the proper response to the challenge using a special hardware or software token.

subnet A network addressing scheme that separates a single network into smaller physical networks.

T

TCP (transmission control protocol) A transport layer networking protocol that provides reliable, ordered delivery of a stream of bytes from one computer to another.

TrustedSource™	A reputation service that reduces spam by filtering incoming mail connections and providing precise information about an e-mail sender's reputation based on its IP address.
Type Enforcement®	A reputation service that reduces spam by filtering incoming mail connections and providing precise information about an e-mail sender's reputation based on its IP address.

U

UDP (user datagram protocol)	A connectionless transport layer protocol that transfers data across a network with no reliability checking or error checking.

V

VLAN interface	An interface that allows administrators to segment a LAN into different broadcast domains regardless of the physical location.
VPN (virtual private network)	A method of authenticating and encrypting data transmissions between hosts (firewall-to-firewall, firewall-to-client). VPN makes it appear as though the remote networks are connected to each other via a pair of routers with a leased line between them.

W

weak authentication	A login process that merely requires a user to enter the same password each time he or she logs in. The "standard" UNIX password process is considered a weak authentication method.

McAfee®