



Application Note

Providing Secure Remote Access to Industrial Control Systems Using McAfee Firewall Enterprise (*Sidewinder*[®])

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

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, MCAFFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

In this document ...

[About this document on page 3](#)

[Deployment scenario on page 4](#)

[Configure the remote access VPN on the corporate firewall on page 7](#)

[Configure the corporate-to-PCN VPN on both firewalls on page 15](#)

About this document

This document describes configuring McAfee Firewall Enterprise (*Sidewinder*) to provide secure remote access to critical control systems for utility, power, energy, water, chemical, and manufacturing industries. It includes an example deployment scenario and a configuration roadmap for configuring two firewalls as depicted in the deployment scenario.

You must install and configure both firewalls before configuring remote access.

Note: This document assumes that you have installed and configured the McAfee Firewall Enterprise that protects the process control network (PCN). Instructions for configuring the PCN McAfee Firewall Enterprise are included in a complementary application note titled *Protecting Industrial Control Systems using McAfee Firewall Enterprise*, available at mysupport.mcafee.com.

Remote access security guidelines

The configuration roadmap in this document addresses the following remote access security guidelines, which have been extracted from publications by the National Institute of Standards and Technology (NIST) and other organizations:

- Do not directly connect process control networks (PCNs) to the Internet, even if protected by a firewall.
- Use virtual private networks (VPNs) to provide secure remote access.
- If your organization prefers to use an access point provided by the corporate network:
 - Require authentication to establish remote access connections.
 - Require users to authenticate a second time using strong two-factor authentication to access the PCN.
- If your organization does not permit unencrypted control traffic to traverse the corporate network, require a secondary tunneling solution, such as an IPsec VPN tunnel, between the remote access point and the destination network (PCN or DMZ).

About the McAfee Firewall Enterprise IPsec VPN solution

The McAfee Firewall Enterprise VPN solution uses the IPsec protocol suite to secure data transmission across unsecured networks through an encryption and decryption process. To increase security, you apply access rules to VPNs in the same way you do for physically connected networks. There are two VPN types:

- **Client-to-gateway** – A VPN connection from a client (usually a user's laptop) to a firewall
- **Gateway-to-gateway** – A VPN connection between one firewall and another firewall

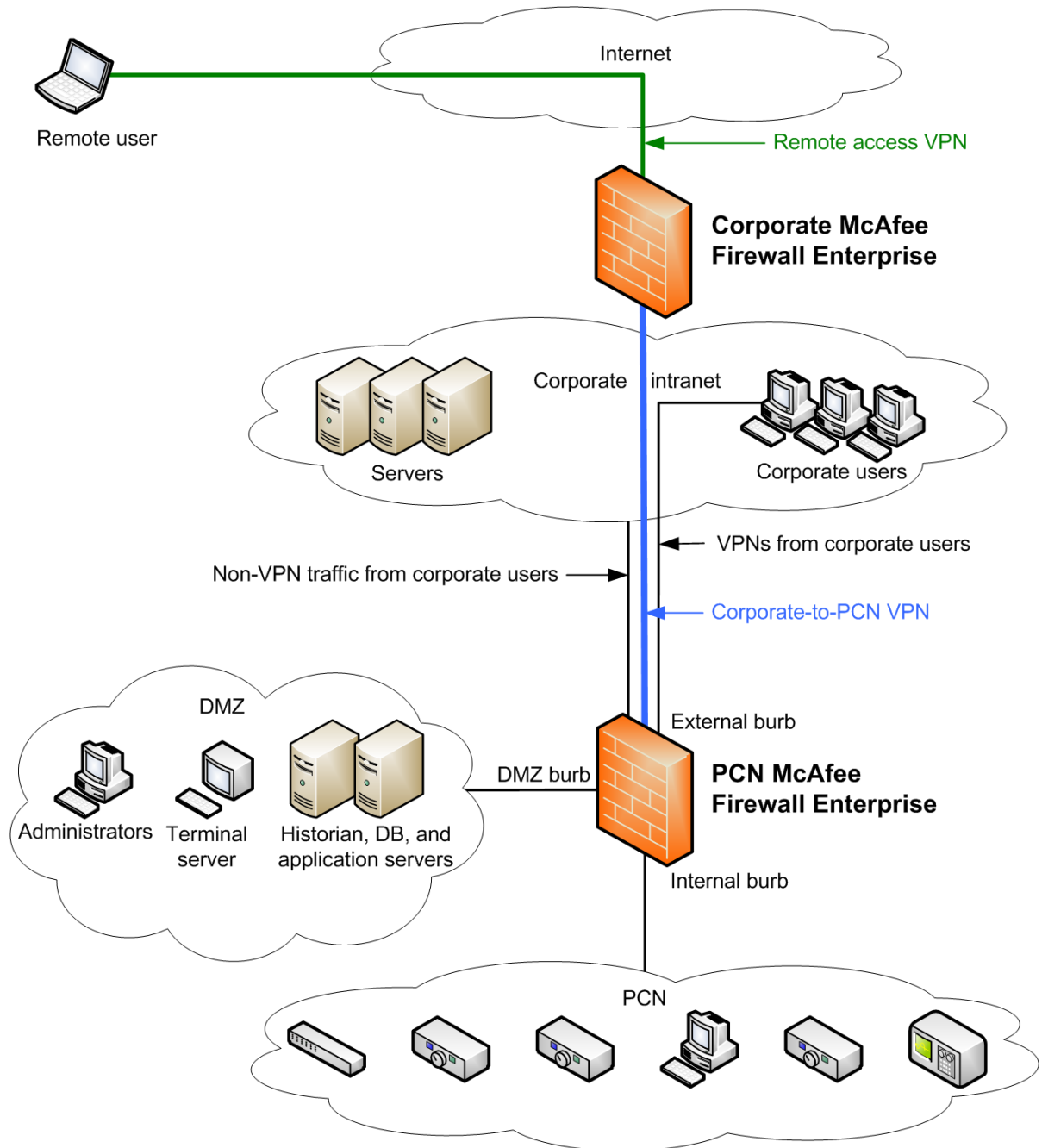
This document contains examples of both gateway-to-gateway and client-to-gateway VPNs.

Note: It is also possible to secure remote access connections using Secure Sockets Layer (SSL) encryption. However, this method is less suited to provide PCN access because protocols must be SSL-aware. Since most industrial control protocols were not created with SSL in mind, this document focuses on IPsec technology.

Deployment scenario

The deployment scenario shown in [Figure 1](#) depicts an example configuration that provides remote access to the PCN in a manner that satisfies the requirements in [Remote access security guidelines on page 3](#). In this scenario, both the corporate and the process control networks are protected by a McAfee Firewall Enterprise.

Figure 1 Deployment scenario



Scenario elements

Firewalls in this scenario:

- **Corporate McAfee Firewall Enterprise** – Protects the corporate network from Internet
- **PCN McAfee Firewall Enterprise** – Protects the PCN and DMZ from the corporate network

VPNs in this scenario:

- **Remote access VPN** – A client-to-gateway VPN that allows remote users to establish a secure connection to the corporate firewall
- **Corporate-to-PCN VPN** – A gateway-to-gateway VPN that allows secure communication between the corporate firewall and the PCN firewall

Connections from remote users reach the PCN by:

- 1 Traversing the remote access VPN
- 2 Traversing the corporate-to-PCN VPN

How VPN traffic flows in this scenario

This deployment scenario employs two VPNs and two virtual burbs to allow remote access to the PCN. To understand how VPN traffic is processed in this scenario, two terms must be defined:

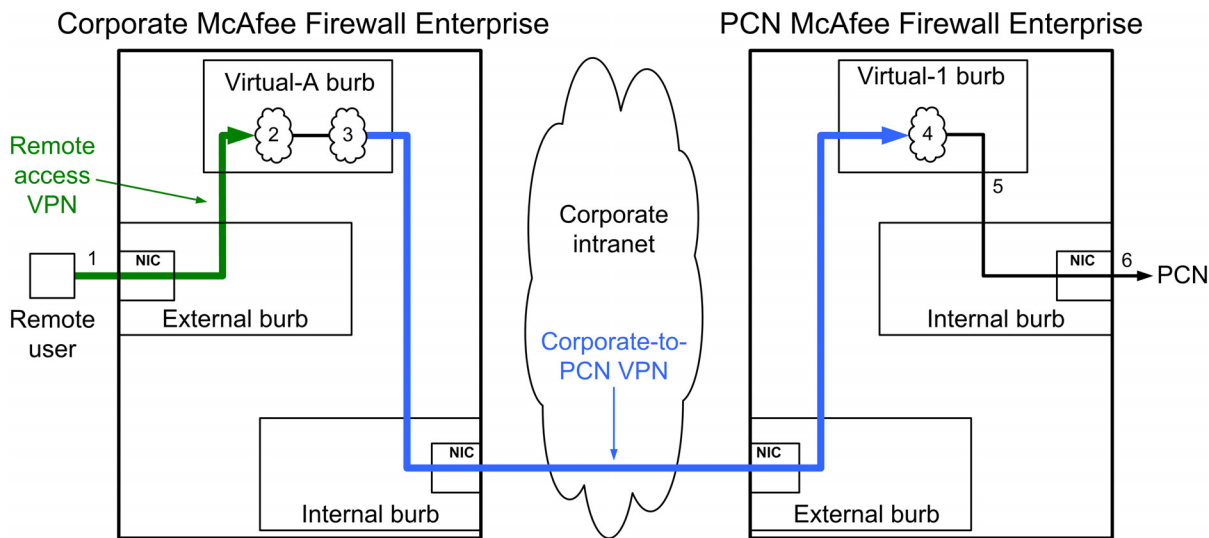
- **Termination burb** – A burb in which VPN traffic transitions between plain-text and encrypted data
- **Virtual burb** – A burb that does not contain a network interface card (NIC), typically used as a VPN termination burb

When configuring a McAfee Firewall Enterprise VPN, using a virtual burb as the VPN termination burb gives you the following benefits:

- VPN traffic is isolated from your physical networks.
- You can enforce access control on traffic that passes through the VPN (policy rules are required to allow traffic to flow from burb to burb).

Figure 2 shows how VPN traffic flows in this deployment scenario: from remote users on the Internet to the PCN network via the corporate and PCN firewalls.

Figure 2 Virtual burb VPN processing



The numbered steps below correspond to the numbers in Figure 2 above.

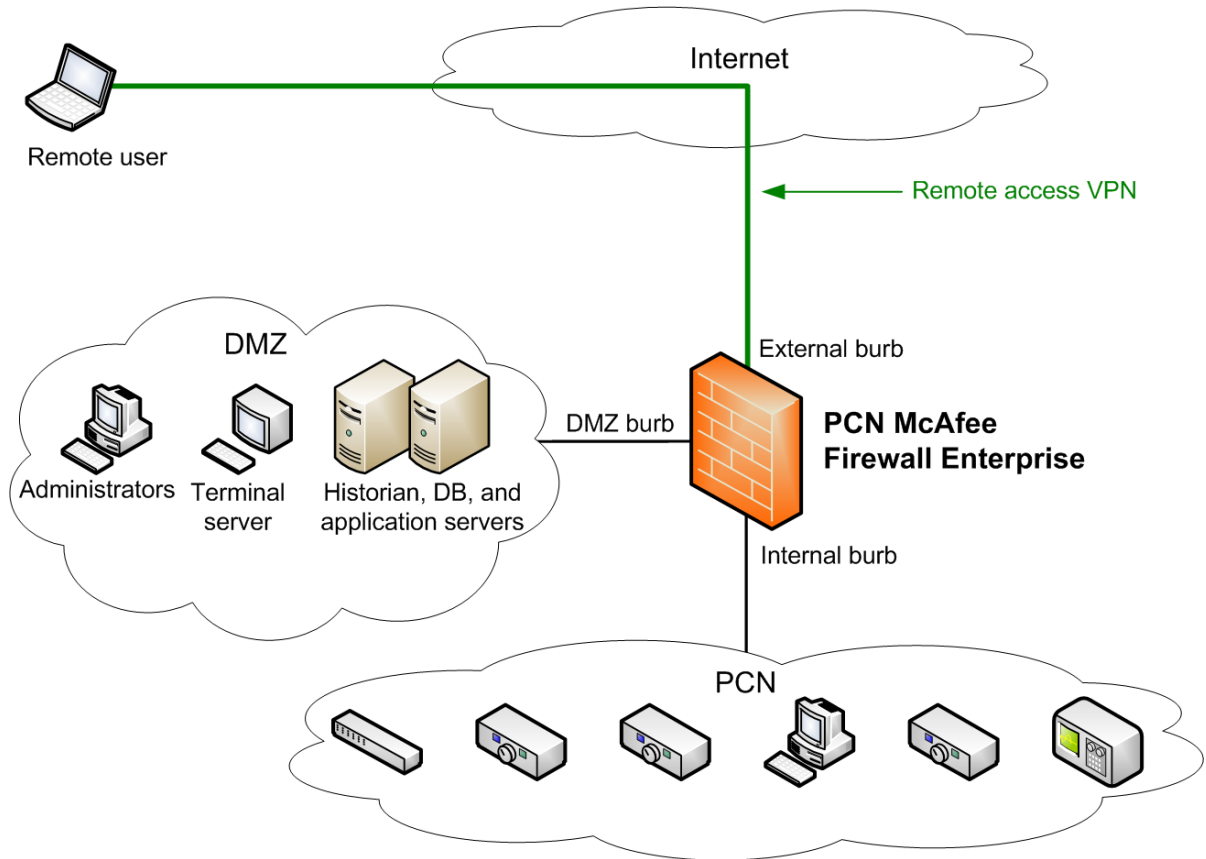
- 1 The remote user initiates a connection to the PCN over the remote access VPN.
- 2 The corporate firewall decrypts the connection in the Virtual-A burb.

- 3 The corporate firewall re-encrypts the connection and forwards it to the PCN firewall.
- 4 The PCN firewall decrypts the connection in the Virtual-1 burb.
- 5 The PCN firewall performs a rule check to allow the connection to leave the Virtual-1 burb.
- 6 The connection reaches the PCN network.

Alternate deployment scenario

While the [Remote access security guidelines on page 3](#) state that PCNs should not be connected to the Internet, even if protected by a firewall, in some cases there may be no other solution. This section describes how you can modify the configuration procedures to allow remote access to DMZ and/or PCN networks via a McAfee Firewall Enterprise that is directly connected to the Internet.

Figure 3 Alternate deployment scenario



To reproduce this configuration:

- 1 Create the remote access VPN on the PCN McAfee Firewall Enterprise. See [Configure the remote access VPN on the corporate firewall on page 7](#).
- 2 Create rules to allow remote users to access the DMZ or PCN as appropriate. See [Create rules on page 19](#) for more information.

Note: Do not perform the configuration procedure in [Configure the corporate-to-PCN VPN on both firewalls on page 15](#).

Configure the remote access VPN on the corporate firewall

This section creates the remote access VPN shown in [Figure 1](#) on the corporate McAfee Firewall Enterprise. This example client-to-gateway VPN provides secure access to the corporate firewall (and by extension, the PCN) to remote users on the Internet.

This VPN has the following attributes:

- Computer identification using self-signed firewall-issued certificates

Note: This configuration is best suited for a small number of remote users because a unique VPN definition must be created for each user. If you have a large number of remote users, consider creating a single VPN definition that uses a Certificate Authority (CA) for remote certificate management.

- User authentication via the extended authentication (XAUTH) method

Tip: While this example configuration uses fixed passwords stored by McAfee Firewall Enterprise, a two-factor authentication method is strongly recommended.

- Simplified client management using a client address pool

Client address pools allow the firewall to assign the following information to the client:

- An IP address for the client's virtual network adapter
- DNS servers that are available to the client
- WINS servers that are available to the client
- VPN termination in a virtual burb named Virtual-A

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

To configure the example client-to-gateway VPN:

- [Set up VPN elements on page 7](#)
- [Create VPN policy for each remote client on page 12](#)

Set up VPN elements

Before you create new VPN definitions, perform the following tasks:

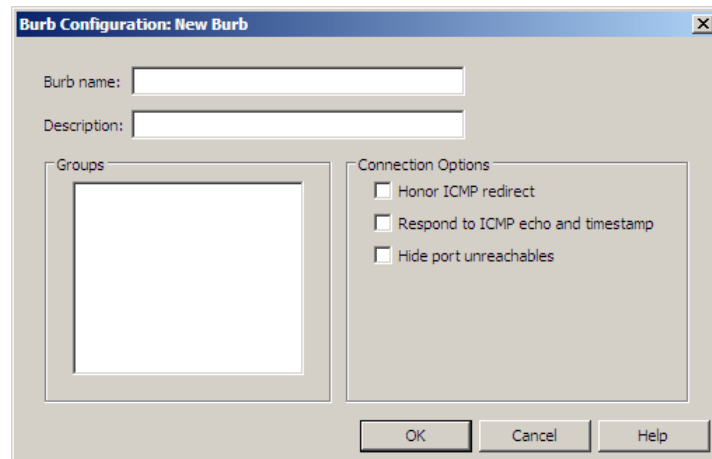
- [Create a virtual burb on page 7](#)
- [Enable extended authentication on the ISAKMP server on page 8](#)
- [Allow access to the ISAKMP server on page 9](#)
- [Create and export a self-signed firewall certificate on page 9](#)
- [Create a client address pool on page 11](#)

Create a virtual burb

Create a virtual burb in which to terminate VPN traffic from remote clients. To create the virtual burb:

- 1 Select **Network > Burb Configuration**.
- 2 Click **New Burb**. The New Burb window appears.

Figure 4 New Burb window



- 3 In the **Burb name** field, enter **virtual-A**.
- 4 Click **OK** and then save your changes.

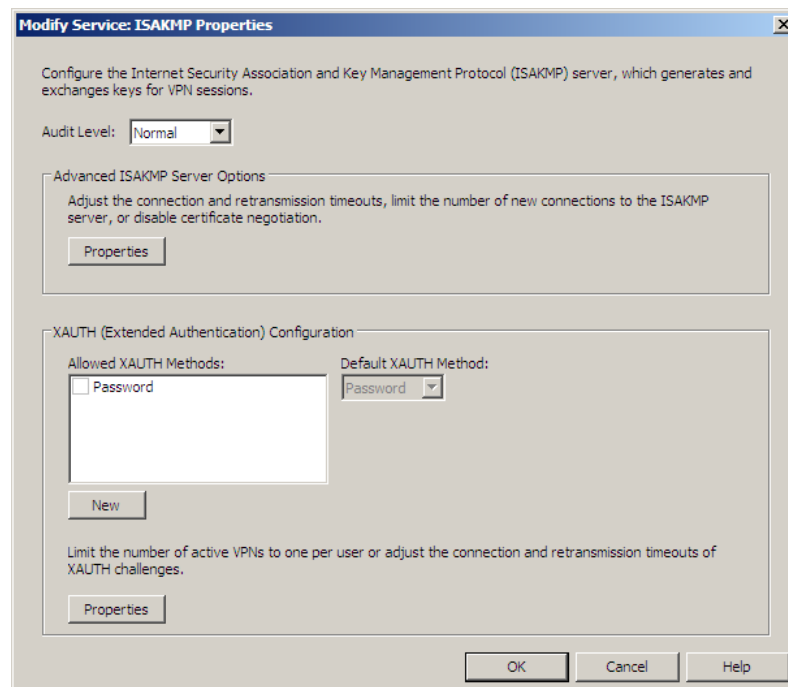
Enable extended authentication on the ISAKMP server

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 5 ISAKMP Properties window



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

Tip: If you want to use a different authentication method for XAUTH, such as Active Directory or RADIUS, click **New** to configure the desired authenticator.

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

Allow access to the ISAKMP server

Create a rule to allow remote clients and the PCN McAfee Firewall Enterprise to access 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** – <Any>
 - **Source Endpoint** – <Any>
 - **Destination Burb** – <Any>
 - **Destination Endpoint** – <Any>
- 3 Save your changes.

Create and export a self-signed firewall certificate

When firewall self-signed certificates are used for VPN authentication, two certificates must be installed on each client: the firewall's self-signed certificate and the client's certificate.

To create and export a self-signed firewall certificate:

- 1 Select **Maintenance > Certificate Management**.
- 2 Select the **Firewall Certificates** tab.
- 3 Create a firewall certificate.
 - a Click **New**. The Create New Certificate window appears.

Figure 6 Create New Certificate window

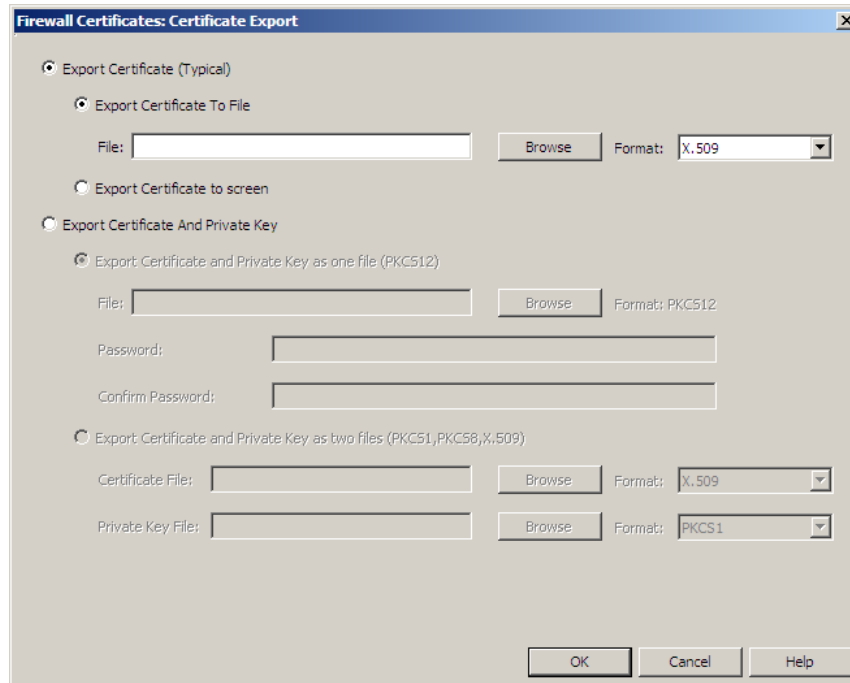
The screenshot shows a dialog box titled "Firewall Certificates: Create New Certificate". It has the following fields and controls:

- Certificate Name:** A text input field.
- Distinguished Name:** A large text area for entering the certificate's distinguished name.
- E-Mail Address:** A text input field.
- Domain Name:** A text input field.
- IP Address:** A text input field with a search icon.
- Submit to CA:** A dropdown menu currently set to "Self Signed".
- Signature type:** Two radio buttons, "RSA" (selected) and "DSA".
- Other Parameters:** A text area currently containing "None".
- Buttons:** "Add", "Close", and "Help" buttons at the bottom right.

- b Configure the following areas:
 - **Certificate Name** – Enter a name of your choosing.
 - **Distinguished Name** – Enter a name appropriate for your firewall.
Example: *CN=Myfirewall,O=mycompany,C=US*
 - **Submit to CA** – Select **Self Signed**.
 - **Signature Type** – Select **RSA**.

- c Click **Add**.
- d Save your changes.
- 4 Export the firewall certificate you created in [Step 3](#).
 - a In the **Certificates** area, select the certificate.
 - b Click **Export**. The Certificate Export window appears.

Figure 7 Certificate Export window



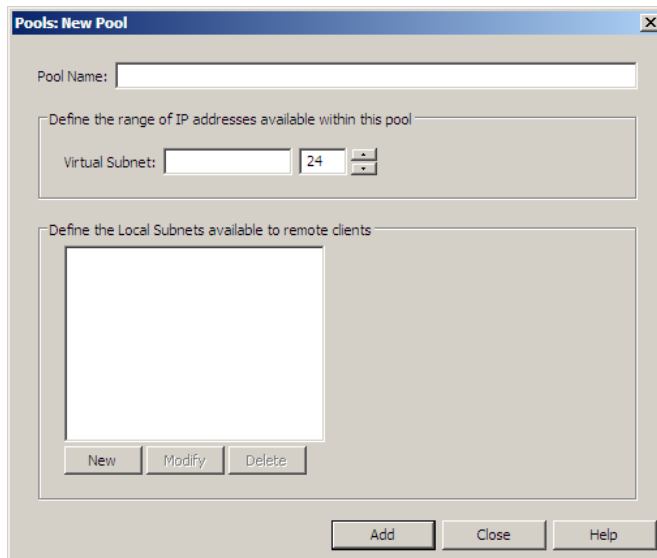
- c Select **Export Certificate to File**.
- d Click **Browse** and specify where you want to save the firewall certificate.
Tip: You can save the firewall certificate to an accessible location (portable storage device or protected network) for distribution to the client.
- e Click **OK**.

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 in the New Pool window:
 - **Pool Name** – Enter a name, such as *Remote_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 DMZ that VPN users will be allowed to access.

Figure 8 New Pool window



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

Create VPN policy for each remote client

For each remote user that requires VPN access, perform the following tasks:

- [Create and export a certificate for the remote client on page 12](#)
- [Create a remote VPN client definition for the client on page 14](#)

Create and export a certificate for the remote client

To create and export a self-signed remote certificate:

- 1 Select **Maintenance > Certificate Management**.
- 2 Select the **Remote Certificates** tab.
- 3 Create a remote certificate.
 - a Click **New**. The Create New Certificate window appears.

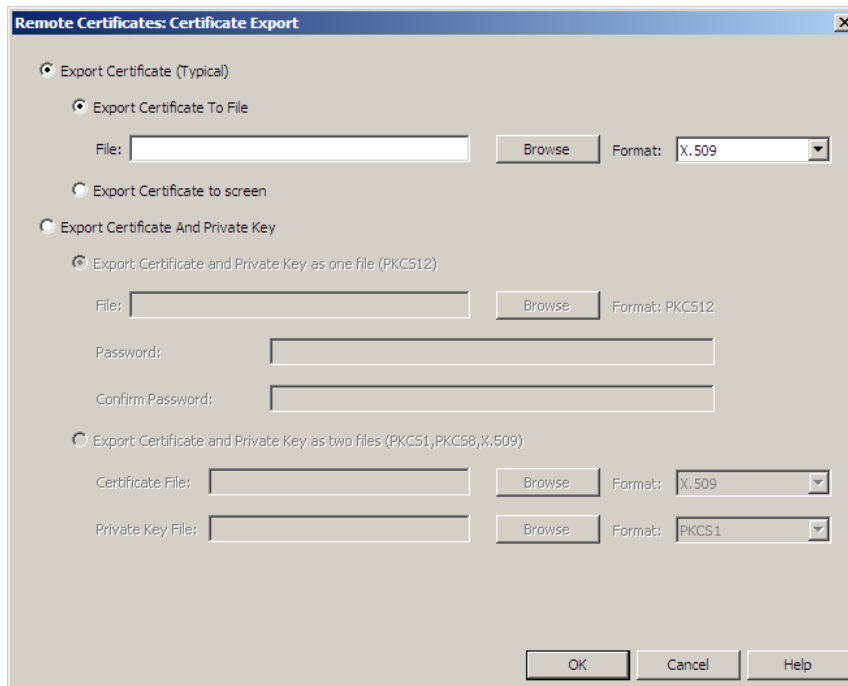
Figure 9 Create New Certificate window

The screenshot shows a dialog box titled "Remote Certificates: Create New Certificate". It has the following fields and controls:

- Certificate Name:** A text input field.
- Distinguished Name:** A large text area for entering a name like `CN=John Doe,O=mycompany,C=US`.
- E-Mail Address:** A text input field.
- Domain Name:** A text input field.
- IP Address:** A text input field with a search icon.
- Submit to CA:** A dropdown menu currently showing "Self Signed".
- Signature type:** Two radio buttons, "RSA" (selected) and "DSA".
- Other Parameters:** A text area containing the word "None".
- Buttons:** "Add", "Close", and "Help" at the bottom right.

- b Configure the following areas:
 - **Certificate Name** – Enter a name of your choosing.
 - **Distinguished Name** – Enter a name appropriate for the user.
Example: `CN=John Doe,O=mycompany,C=US`
 - **Submit to CA** – Select **Self Signed**.
 - **Signature Type** – Select **RSA**.
 - c Click **Add**.
 - d Save your changes.
- 4 Export the remote certificate you created in [Step 3](#).
 - a In the **Certificates** area, select the certificate.
 - b Click **Export**. The Certificate Export window appears.

Figure 10 Certificate Export window



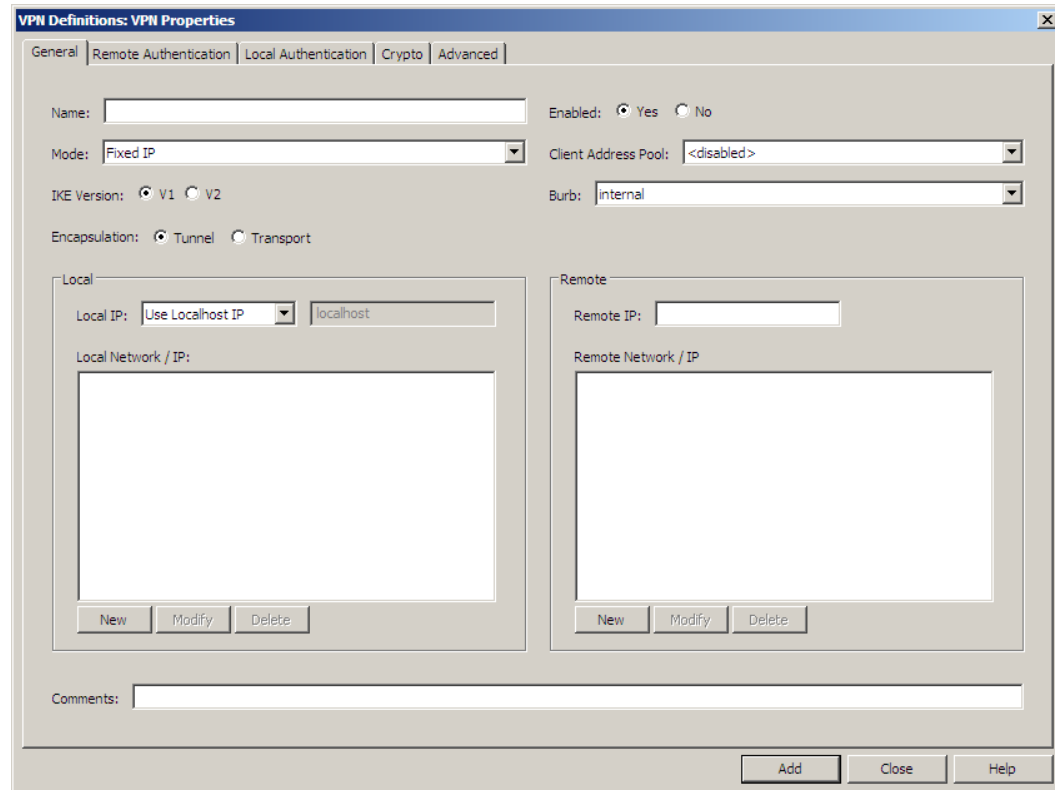
- c** Select **Export Certificate And Private Key**.
- d** Select **Export Certificate And Private Key as one file (PKCS12)**.
- e** Click **Browse** and specify where you want to save the remote certificate.
Tip: You can save the remote certificate to an accessible location (portable storage device or protected network) for distribution to the client.
- f** In the **Password** field, type a password to protect the file.
- g** In the **Confirm Password** field, re-type the password.
- h** Click **OK**.

Create a remote VPN client definition for the client

To create a VPN definition:

- 1 Select **Network > VPN Configuration > VPN Definitions**, and then click **New**. The VPN Properties window appears.

Figure 11 VPN General tab



- 2 On the **General** tab, specify the following:
 - **Name** – Remote_User_username
Tip: Include the user name of the remote user that will be using this VPN.
 - **Mode** – Dynamic IP Restricted Client
 - **IKE version** – V1
 - **Encapsulation** – Tunnel
 - **Enabled** – Yes
 - **Client Address Pool** – Remote_Users_Pool
 - **Burb** – Virtual-A
 - **Local IP** – Use Localhost IP
- 3 On the **Remote Authentication** tab, specify the following:
 - **Remote Authentication Method** – XAUTH + Single Certificate
 - **Remote Certificate** – Select the certificate you created for the remote user in [Create and export a certificate for the remote client on page 12](#).
- 4 On the **Local Authentication** tab, specify the **Local Certificate** – Select the firewall certificate you created in [Create and export a self-signed firewall certificate on page 9](#).
- 5 Click **Add** and then save your changes.

Configure the corporate-to-PCN VPN on both firewalls

This section creates the corporate-to-PCN VPN shown in [Figure 1](#). This example gateway-to-gateway VPN encrypts network traffic that passes between the two firewalls. This ensures that traffic from the remote client VPNs that is destined for the PCN remains secure as it passes through the corporate network on its way to the PCN firewall.

This VPN has the following attributes:

- Computer identification by shared secret (also referred to as password)
- VPN termination in a virtual burbs on both firewalls to enforce access control

To configure the example gateway-to-gateway VPN:

- [Configure the corporate McAfee Firewall Enterprise on page 15](#)
- [Configure the PCN McAfee Firewall Enterprise on page 17](#)

Configure the corporate McAfee Firewall Enterprise

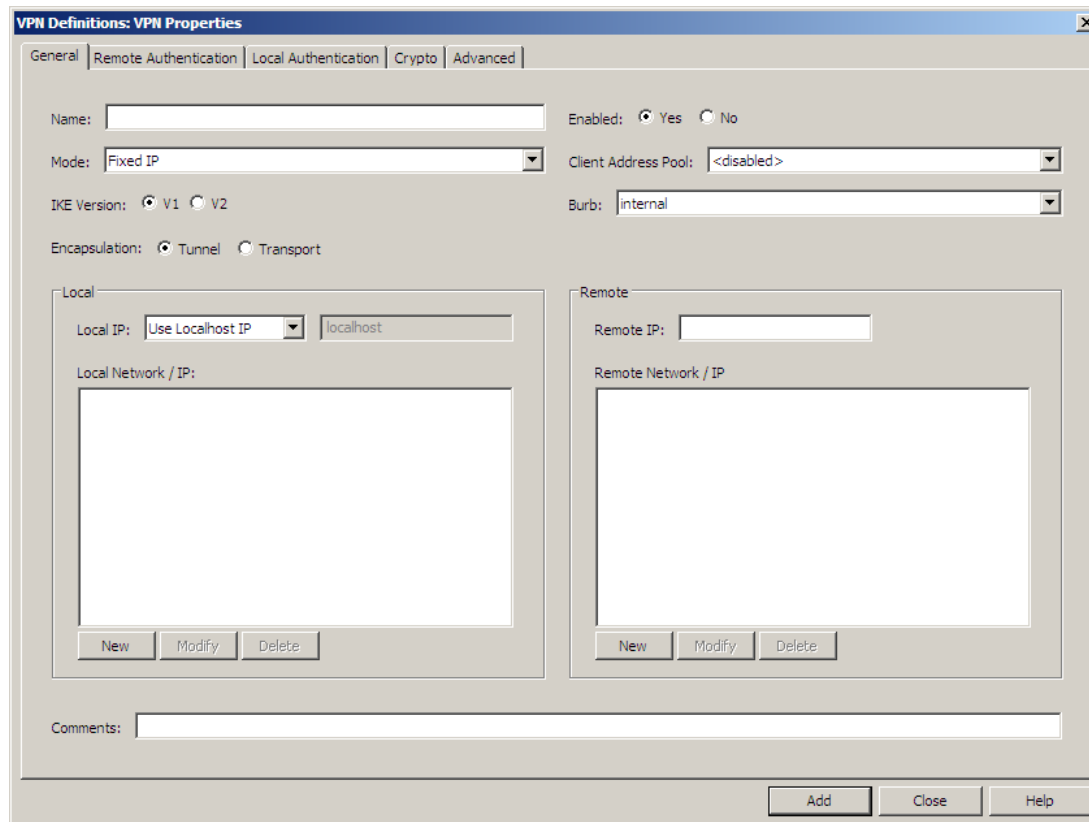
This section configures the corporate-to-PCN VPN on the corporate McAfee Firewall Enterprise.

Note: The ISAKMP server must be configured and a rule created to allow access to it in order to proceed. If you did not perform these tasks in [Configure the remote access VPN on the corporate firewall on page 7](#), do so now.

To configure the VPN definition:

- 1 Select **Network > VPN Configuration > VPN Definitions**, and then click **New**. The VPN Properties window appears.

Figure 12 VPN General tab



- 2 On the **General** tab, specify the following:
 - **Name** – Corporate-to-PCN
 - **Mode** – Fixed IP
 - **IKE version** – V1
 - **Encapsulation** – Tunnel
 - **Enabled** – Yes
 - **Client Address Pool** – <disabled>
 - **Burb** – Virtual-A
 - **Local IP** – Use Localhost IP
 - **Local Network / IP** – Specify the network(s) that you assigned to the Remote_Users_Pool client address pool in [Create a client address pool on page 11](#).
 - **Remote IP** – Type the external IP address of the PCN McAfee Firewall Enterprise.
 - **Remote Network / IP** – Specify the network(s) in the DMZ that remote users will be allowed to access.
- 3 On the **Remote Authentication** tab, specify the following:
 - **Remote Authentication Method** – Password
 - **Enter Remote Password** – Type a password.
 - **Verify Remote Password** – Confirm the password.
 - **Remote Identity** – Gateway IP Address
- 4 On the **Local Authentication** tab, specify the following:
 - **Local Identity Type** – IP Address
 - **Value** – localhost
- 5 Click **Add** and then save your changes.

Configure the PCN McAfee Firewall Enterprise

This section configures the corporate-to-PCN VPN on the PCN McAfee Firewall Enterprise.

To configure the VPN:

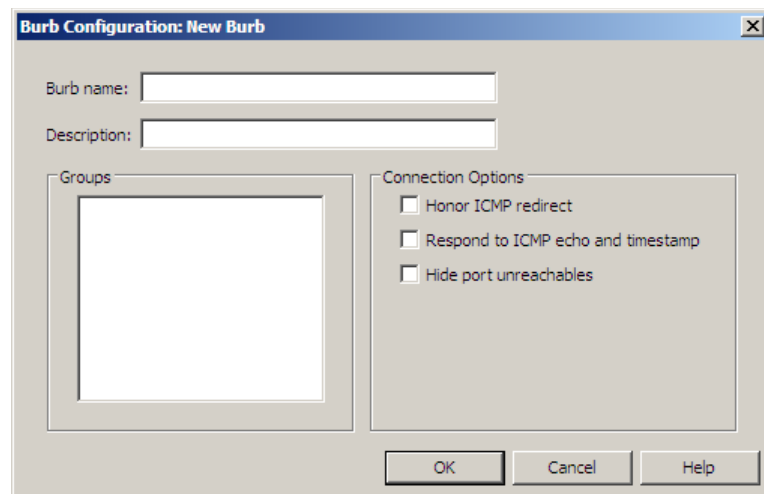
- [Create a virtual burb on page 17](#)
- [Allow access to the ISAKMP server on page 17](#)
- [Create the VPN definition on page 18](#)
- [Create rules on page 19](#)

Create a virtual burb

Create a virtual burb in which to terminate VPN traffic from the corporate McAfee Firewall Enterprise. To create the virtual burb:

- 1 Select **Network > Burb Configuration**.
- 2 Click **New Burb**. The New Burb window appears.

Figure 13 New Burb window



- 3 In the **Burb name** field, enter **Virtual-1**.
- 4 Click **OK** and then save your changes.

Allow access to the ISAKMP server

Create a rule to allow the corporate McAfee Firewall Enterprise to access 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** – <Any>
 - **Destination Burb** – external
 - **Destination Endpoint** – <Any>
- 3 Save your changes.

Create the VPN definition

To configure the VPN definition:

- 1 Select **Network > VPN Configuration > VPN Definitions**, and then click **New**. The VPN Properties window appears.

Figure 14 VPN General tab

The screenshot shows the 'VPN Definitions: VPN Properties' dialog box with the 'General' tab selected. The 'Name' field is empty. The 'Mode' is set to 'Fixed IP'. 'IKE Version' has 'V1' selected. 'Encapsulation' has 'Tunnel' selected. 'Enabled' has 'Yes' selected. 'Client Address Pool' is set to '<disabled>'. 'Burb' is set to 'internal'. The 'Local' section has 'Local IP' set to 'Use Localhost IP' and 'localhost'. The 'Remote' section has 'Remote IP' empty. Both sections have empty lists for 'Local Network / IP' and 'Remote Network / IP'. At the bottom, there is a 'Comments' field and 'Add', 'Close', and 'Help' buttons.

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

- **Name** – Corporate-to-PCN
- **Mode** – Fixed IP
- **IKE version** – V1
- **Encapsulation** – Tunnel
- **Enabled** – Yes
- **Client Address Pool** – <disabled>
- **Burb** – Virtual-1
- **Local IP** – Use Localhost IP
- **Local Network / IP** – Specify the network(s) in the DMZ that remote users will be allowed to access.
- **Remote IP** – Type the internal IP address of the corporate McAfee Firewall Enterprise.
- **Remote Network / IP** – Specify the network(s) that you assigned to the Remote_Users_Pool client address pool in [Create a client address pool on page 11](#).

- 3 On the **Remote Authentication** tab, specify the following:
 - **Remote Authentication Method** – Password
 - **Enter Remote Password** – Type a password.
 - **Verify Remote Password** – Confirm the password.
 - **Remote Identity** – Gateway IP Address
- 4 On the **Local Authentication** tab, specify the following:
 - **Local Identity Type** – IP Address
 - **Value** – localhost
- 5 Click **Add** and then save your changes.

Create rules

Create rules to allow VPN traffic to leave the Virtual-1 burb and reach its final destination. These rules should have the following general characteristics:

- **Source Burb** – Virtual-1
- **Source Endpoint** – A network object containing the client address pool network(s) you specified in [Create a client address pool on page 11](#)
- **Destination Burb** – DMZ or PCN burbs as necessary

For more information on creating rules, refer to the following documents at mysupport.mcafee.com:

- *Protecting Industrial Control Systems Using McAfee Firewall Enterprise (Sidewinder)*
- *McAfee Firewall Enterprise Administration Guide*

Configure the corporate-to-PCN VPN on both firewalls

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.

