TECHNICAL WHITE PAPER

Symantec pcAnywhere™ Security Recommendations

Symantec

Technical White Paper

Symantec pcAnywhere™ Security Recommendations

Introduction

At this time, Symantec recommends that customers ensure pcAnywhere 12.5 is installed, apply all relevant patches as they are released, and follow general security best practices. If customers are unable to adhere to this guidance and have not installed the latest version with current patches, we recommend that they contact pcanywhere@symantec.com for additional assistance.

On Monday, January 23, 2012, Symantec released a patch that eliminates known vulnerabilities affecting customers using pcAnywhere 12.5. An update to this patch to support pcAnywhere 12.0 and pcAnywhere 12.1 is planned for release on Friday January 27, 2012.

This document is designed to help customers understand how to address the issues based on their specific use case and implement best practices to maintain the protection of their devices and information.

pcAnywhere Configuration Recommendations

Remote control products provide significant flexibility to accommodate a variety of connection scenarios. As a result it is important that every customer understand these scenarios and configure the product to meet their own internal security standards. The following best practices are recommended and should be applied according to the scenario that best fits the requirement of the specific environment. It is important that these best practices be read in conjunction with the specific risk scenarios outlined in the next section before determining a course of action for a given environment. Symantec is not recommending that any one specific action will provide a solution for an environment but rather applying a combination of pcAnywhere security best practices along with the above general security best practices.

Update to Latest Version of pcAnywhere

Customers should update pcAnywhere to the latest version of pcAnywhere (12.5), and install the latest patches. Information on obtaining current hotfixes for supported versions is available online at http://www.symantec.com/docs/TECH179526.

Block Default Ports on Corporate Firewalls

Customers should block pcAnywhere assigned ports (5631, 5632) on Internet facing network connections, or shut off port forwarding of these ports. Blocking these ports will help ensure that an outside entity will not have access to pcAnywhere through these ports, and will help ensure that the use of pcAnywhere remains within the confines of the corporate network.

Tune the Host Behavior for Roaming Users

By default, the Host is configured not to listen for a connection. Many organizations often modify this setting so that the Host is always set to listen. Our recommendation is to verify what setting is currently in place. If you have selected the option to always listen it is recommended that you turn this feature off. In addition it is also good practice to set the Hosts not to run until needed. Configuring these setting limits the exposure of active pcAnywhere agents within the corporate network.

To stop the pcAnywhere services on a roaming system, or following a remote session, the following script can be used:

```
@echo off
REM: Disable pcAnywhere host, and set startup to disabled
net stop awhost32
sc config awhost32 start= disabled
```

To restart the service prior to a remote session, the following script can be executed (once the session is complete the service should be stopped again, using the script above):

```
@echo off
REM: Start the pcAnywhere host to allow for a remote session
sc config awhost32 start= auto
net start awhost32
```

These scripts can be executed remotely using a job or task within Symantec IT Management Suite (ITMS) or through a similar tool.

Network Security

Network security is a critical area when implementing remote control solutions. You may leverage the pcAnywhere Remote Access Perimeter Scanner to identify unexpected hosts. Lastly, you should routinely review the network activity logs for port scans.

Connection Security

When making connections there are a few key recommendations.

- Allow only authorized IP addresses to connect to host sessions, this will cause the client to reject all connection requests that are not authorized.
- Require user acceptance of remote control sessions (not enabled by default) to ensure the user knows that a session is occurring.
- Modify the assigned TCP/IP data and status ports were applicable to ports other than 5631 and 5632. This makes it a little more difficult to locate machines running pcAnywhere in your environment.
- Use encryption to protect communication within a pcAnywhere session, this is not set by default so this ensures that it is hard for anyone to see session data.
- Use pcAnywhere authentication as opposed to WinNT or Active Directory in order to limit exposure of Windows or Active Directory credentials.
- Logoff host on connect in order to force users to authenticate to Windows or AD in order to start a remote session.
- Reboot host on disconnect in order to ensure that a system is not left in a logged-in state following a remote session.
- Limit the number of login attempts in order to protect against brute force attacks locking remote access to the machine after a minimum of three attempts.
- Disable docking to Access Server with public facing IP addresses since it is recommended that secure VPN tunnels be used in these situations.

Apply Changes to Configuration Files

Once the above pcAnywhere connection security settings are made, they should be applied to all systems as quickly as possible. For users of pcAnywhere Solution, which is included in Altiris Client Management Suite or IT Management Suite, these changes will be applied to all systems as soon as the clients update their policies. For pcAnywhere standalone users, the pcAnywhere configuration files (C:\Program Data\Symantec\pcAnywhere*.*) should be copied down to the same location on each client system (using a script or tool such as Symantec ITMS).

Disconnected Users

Disconnected users should be informed to stop the pcAnywhere service or to connect their system to the network in order to apply the required changes. The most efficient method used to apply changes to disconnected users will vary by environment.

Access Server

To limit risk from external sources, customers should host remote sessions via secure VPN tunnels, instead of using pcAnywhere Access Server. When using secure VPN tunnels, it is recommended that Client Management Suite and IT Management Suite customers modify policies relying on pcAnywhere Access Server.

It should be noted that in less common cases where pcAnywhere Access Server is being used within a corporate network, and the Access Server does not use a public facing IP address or require open pcAnywhere ports, it can be used securely within the environment.

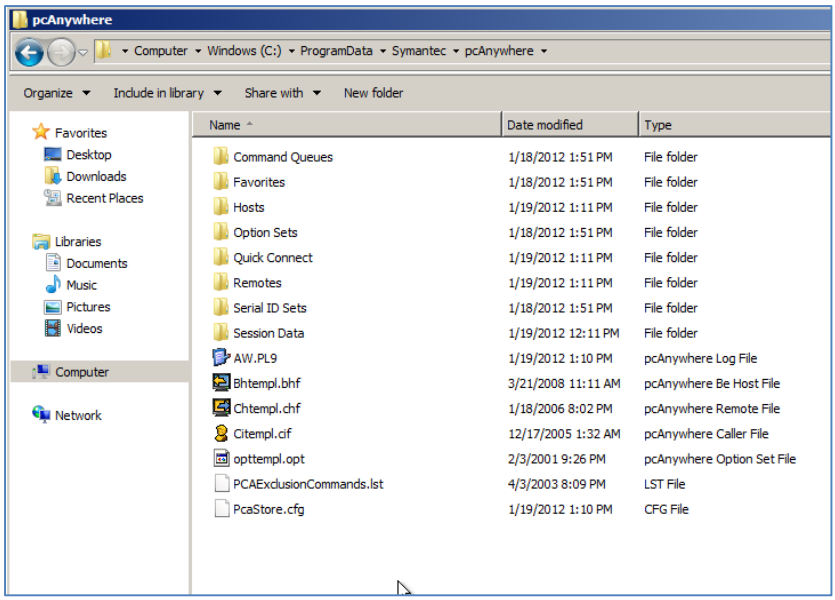
Log Review

Altiris Client Management Suite and IT Management Suite customers should review pcAnywhere reports within the Symantec Management Console. For pcAnywhere standalone, users should enable and review logs for pcAnywhere on a centralized server.

Administrators should review reports and logs for suspicious activities, or unauthorized access, which require further investigation. Active reviewing of logs and reports can help administrators identify network issues as soon as they occur, and react accordingly.

Apply File Security

It is recommended that administrators limit access to the pcAnywhere configuration files (shown below) in order to protect against unauthorized access to pcAnywhere configuration settings.


pcAnywhere
Computer ▸ Windows (C:) ▸ ProgramData ▸ Symantec ▸ pcAnywhere
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Command Queues 1/18/2012 1:51 PM File folder
Favorites 1/18/2012 1:51 PM File folder
Hosts 1/19/2012 1:11 PM File folder
Option Sets 1/18/2012 1:51 PM File folder
Quick Connect 1/19/2012 1:11 PM File folder
Remotes 1/19/2012 1:11 PM File folder
Serial ID Sets 1/18/2012 1:51 PM File folder
Session Data 1/19/2012 12:11 PM File folder
AW.PL9 1/19/2012 1:10 PM pcAnywhere Log File
Bhtempl.bhf 3/21/2008 11:11 AM pcAnywhere Be Host File
Chtempl.chf 1/18/2006 8:02 PM pcAnywhere Remote File
Citempl.cif 12/17/2005 1:32 AM pcAnywhere Caller File
opttempl.opt 2/3/2001 9:26 PM pcAnywhere Option Set File
PCAExclusionCommands.lst 4/3/2003 8:09 PM LST File
PcaStore.cfg 1/19/2012 1:10 PM CFG File

General Security Best Practices

Implementing security best practices minimizes the inherent risks as a result of the incident. Symantec recommends that customers review their current policies in the following areas:

- Endpoint Security: Customers should verify that anti-virus and firewall technologies are installed on all host systems and that the most current definition files are up to date.
- Network Security: Customers should have current and updated perimeter firewalls, email/web security gateways and intrusion detection systems in place. Insecure ports should be disabled and source/destination access should be restricted if port forwarding or network translation is enabled for pcAnywhere access.
- Remote Access Security: For remote users using a variety of internal corporate services, connecting through an IPSec or SSL VPN to the corporate network helps ensure that all traffic is encrypted and protected from eavesdropping.
- Physical Security: Any corporate IT server asset should be deployed in a facility or location that is safeguarded against unauthorized entry and access.

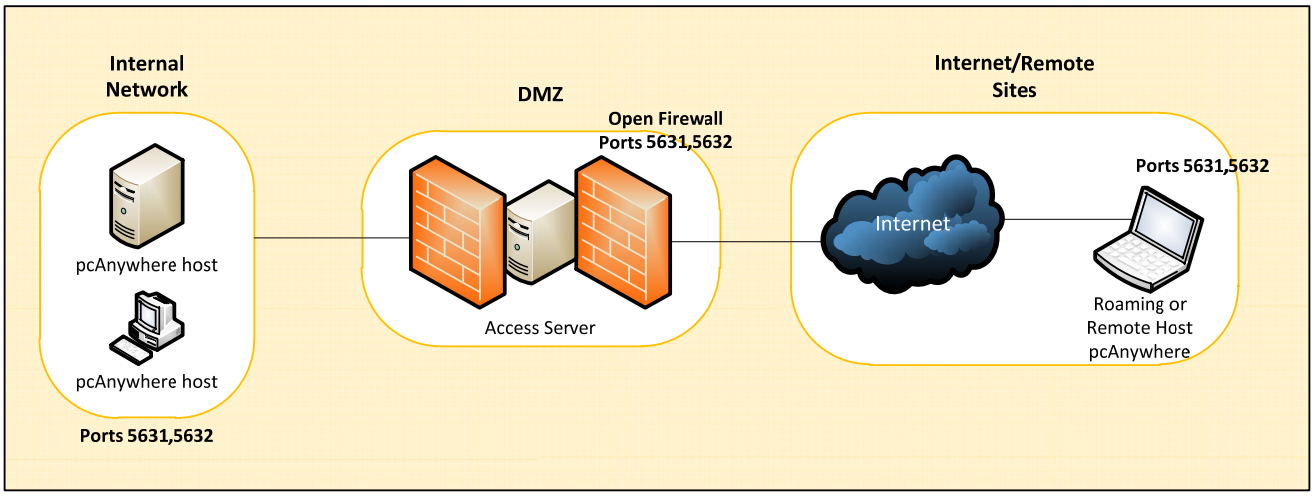
Implementation Best Practices

The following scenarios provide context around the best practices as discussed in the previous section. It is recommended that each scenario be considered and used to determine what is applicable for your environment. It is suggested that you review the best practices in each scenario to help determine what needs to be addressed in that environment.

Symantec also recommends that each customer evaluate their existing security procedures and pcAnywhere configuration to assess and weigh any security risks.

Scenario 1: Mid-Size to Large Environments

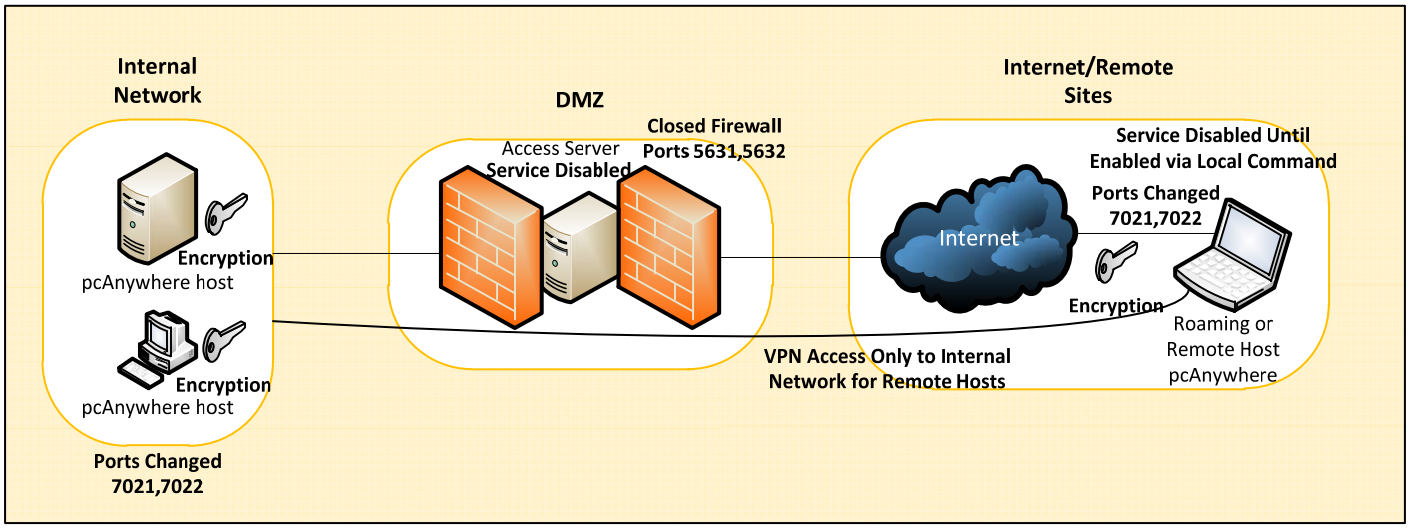
In this scenario machines can be accessed externally through the firewall via the Access Server, or via a direct connection.



Symantec recommends applying the following settings to this environment. To modify the settings refer to the recommendations in the previous section.

- Block the default ports on the firewalls
- Apply Network Security practices
- Apply Connection Security settings
- Apply Changes to Configuration Files
- Apply Access Server settings
- Apply Log Review settings
- Apply File Security

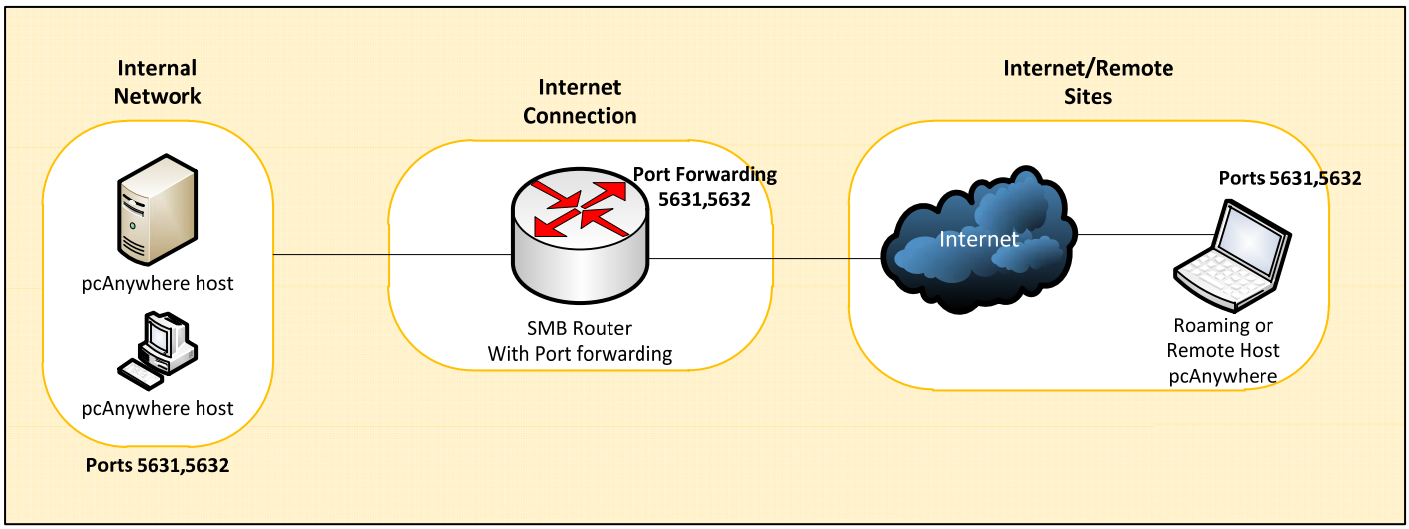
The following diagram depicts the environment changes that would be expected.



NOTE: Port numbers listed above (i.e. 7021 and 7022) are not necessarily the ones that should be chosen; the actual ports selected are at the discretion of the network administrator.

Scenario 2: SMB Environments

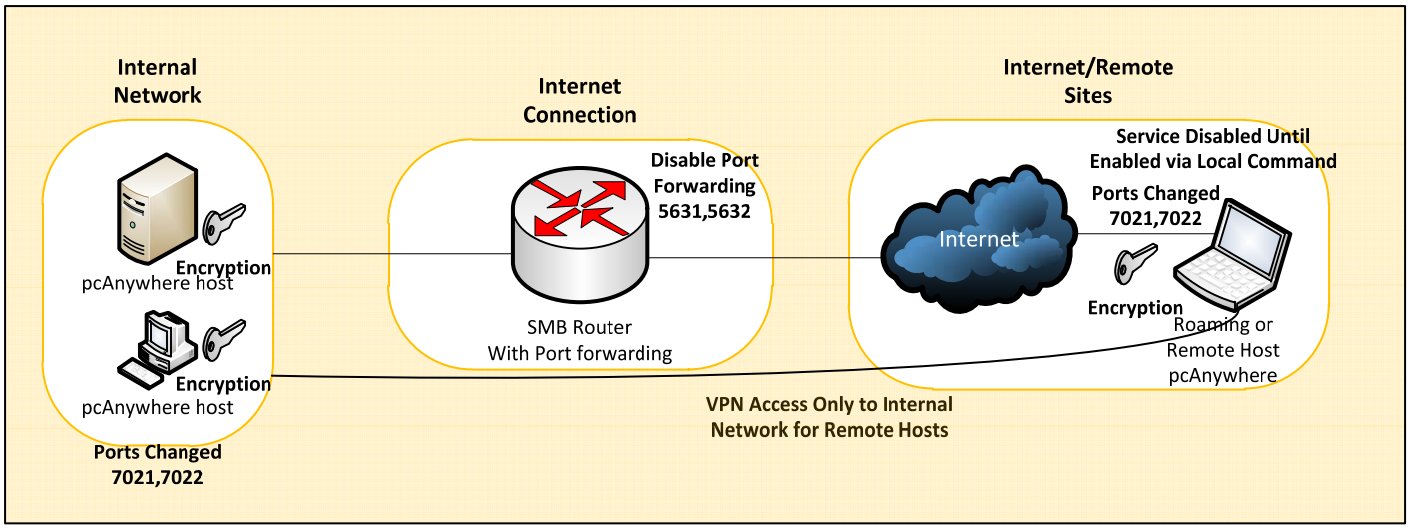
In this scenario machines can be accessed externally through port forwarding, or via a direct connection.



Symantec recommends applying the following settings to this environment. To modify the settings refer to the recommendations in the previous section.

- Use a secure VPN connection for remote sessions
- Disable port forwarding for ports 5631 and 5632 on the SMB Router
- Apply Connection Security settings
- Apply Changes to Configuration Files
- Apply Log Review settings
- Apply File Security

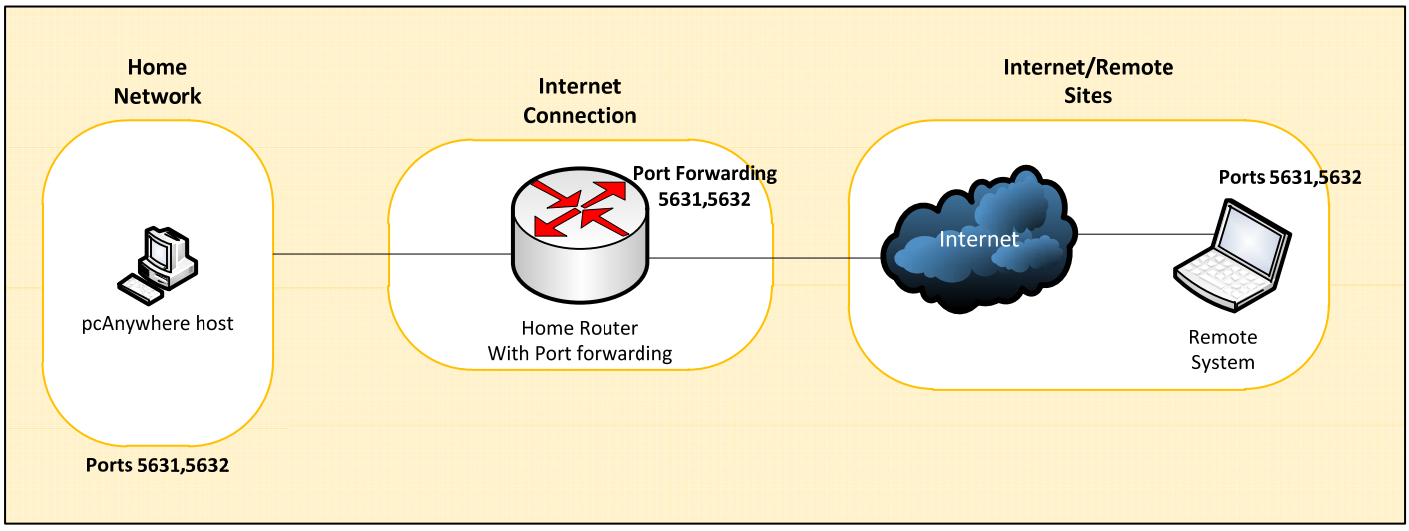
The following diagram depicts the environment changes that would be expected.



NOTE: Port numbers listed above (i.e. 7021 and 7022) are not necessarily the ones that should be chosen; the actual ports selected are at the discretion of the network administrator.

Scenario 3: Consumer Environments

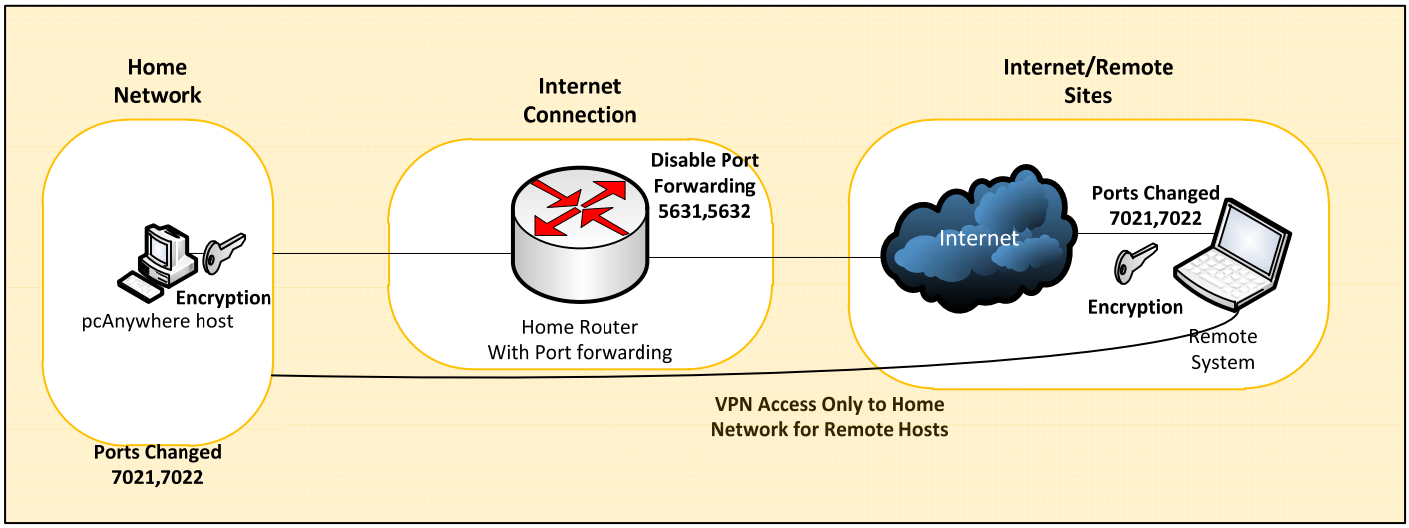
In this scenario machines can be accessed externally through port forwarding, or via a direct connection.



Symantec recommends applying the following settings to this environment. To modify the settings refer to the recommendations in the previous section.

- Use a secure VPN connection for remote sessions
- Disable port forwarding for ports 5631 and 5632 on the SMB Router
- Apply Connection Security settings
- Apply Log Review settings
- Apply File Security

The following diagram depicts the environment changes that would be expected.



NOTE: Port numbers listed above (i.e. 7021 and 7022) are not necessarily the ones that should be chosen; the actual ports selected are at the discretion of the network administrator.

Resources

Online Product Support Information

Customers may access support information related to both pcAnywhere and pcAnywhere Solution on symantec.com:

pcAnywhere: http://www.symantec.com/business/support/index?page=landing&key=52418
pcAnywhere Solution: http://www.symantec.com/business/support/index?page=landing&key=57807

User Documentation

In addition it is recommended that customers review the user documentation to understand how to modify and configure the product. Chapter 9 of the user guide describes the security options.
http://www.symantec.com/docs/DOC4459

Important Knowledge Base Articles

New Knowledge Base articles have been posted to assist customers with locating, updating, removing or disabling pcAnywhere.

- Information on obtaining current hotfixes for supported versions: http://www.symantec.com/docs/TECH179526
- pcAnywhere Automated Uninstall Procedures: http://www.symantec.com/docs/HOWTO65761
- How to disable pcAnywhere: http://www.symantec.com/docs/HOWTO65768
- How to block pcAnywhere executables in Windows 2008 Domain Controller GPO: http://www.symantec.com/docs/HOWTO65791
- How to block pcAnywhere executables in Windows 2003 Domain Controller GPO: http://www.symantec.com/docs/HOWTO65792

General Security Guidelines

Symantec Security Best Practices for Stopping Malware and Other Threats
http://www.symantec.com/theme.jsp?themeid=stopping_malware

National Institute for Standards and Technology Engineering Principles for Information Technology Security
http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation

World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

1 (800) 721 3934

www.symantec.com