

Managing external connections using Symantec pcAnywhere

Symantec pcAnywhere supports TCP/IP network connections over a local area network (LAN), wide area network (WAN), or the Internet. To establish a connection with a host, pcAnywhere must be able to determine the IP address and port number of the host computer. If the host and remote computers are attached to the same network and are using the default pcAnywhere ports, establishing a connection is straightforward. The remote user can either specify the IP address of the host or browse one or more subnets for all advertised pcAnywhere hosts that are waiting for a connection. The session begins once the host computer validates the authentication credentials sent by the remote user.

Connecting to a host computer that is behind a firewall or that has a hidden IP address from outside the network poses a challenge. The security mechanisms that are designed to protect network resources from unauthorized access can also limit a remote user's ability to access the network for legitimate business purposes. Another challenge arises when the remote user must connect by modem but needs to reach a network computer that does not have a modem. To make the connection, the remote user must be able to connect through a gateway or other device capable of handling the translation.

Why the pcAnywhere gateway is no longer supported

Early versions of pcAnywhere let administrators configure a host computer on the network to serve as a gateway between modem and network connections. The pcAnywhere gateway enabled all users within the network to share a single modem. The pcAnywhere gateway handled the translation between the TAPI or CAPI communications protocols and TCP/IP, enabling one-way and two-way communications between these devices. Users within the network who did not have modem access could connect to other modems (for example, access a bulletin board system [BBS]) via the gateway, and modem users outside the network could connect to network users within the network via the gateway. Technological advances in networking, the advent of virtual private networks (VPN) and remote access servers (RAS), and growing security concerns about controlling access to the network through modems are some of the factors that influenced Symantec's decision to stop supporting the pcAnywhere gateway.

Resolving the remote access challenge

Administrators commonly face the following challenges when implementing pcAnywhere or other remote access solutions:

- A firewall that is configured to block pcAnywhere ports
- A Network Address Translation (NAT) or router environment in which the host computers that are connected to the device do not have a public IP address
- A remote computing environment in which mobile, dial-in users need to connect to one or more network hosts (dial-in, network-out connections)

Symantec pcAnywhere lets administrators leverage the security mechanisms already in place on their networks to ensure a secure remote computing environment. The most effective and secure solution for providing remote access to the network involves implementing pcAnywhere in conjunction with a VPN or RAS solution. Once the remote user connects through one of these trusted services, the remote computer becomes a node on the network and can easily access the target system.

Firewall solutions

A firewall limits a network’s exposure to unauthorized access by limiting the number of external, inbound entry points. Computers inside the firewall remain hidden from any computer that is outside the firewall. For a remote user outside the firewall to connect to a host computer inside the firewall using pcAnywhere, the network must be configured to allow inbound and outbound traffic on the pcAnywhere ports.

For a growing number of organizations, exposing additional entry points to their network for remote access is a security concern, and administrators are hesitant to open access to the pcAnywhere ports. In this scenario, the following solution is recommended.

Challenge	Solution
Firewall is configured to block pcAnywhere ports.	Adopt a VPN solution combined with Symantec pcAnywhere. <ul style="list-style-type: none">■ The remote user connects to the network using a trusted VPN.■ The remote user then starts pcAnywhere.■ The remote user then connects to the host, either specifying the host IP address or browsing the network for available hosts.

Network Address Translation and router solutions

Network Address Translation (NAT) is a technology that lets multiple computers within a private network access the Internet by sharing a single, routable IP address. NAT is increasing in popularity, especially among small business and home users, because of the scarcity and cost prohibitiveness of registered IP addresses. NAT provides a basic level of security because it makes it possible to limit the number of addresses that access the Internet, thus decreasing a network’s exposure.

In this environment, all inbound and outbound communications between a computer within the private network and the Internet are routed through a NAT device, which handles the address substitution, IP address and port mapping, and message routing. For this reason, remote access to computers within the private network from outside the network presents a challenge. Host computers within the private network are hidden from the outside world. Remote users can connect to the NAT device using the external IP address. However, because the remote user cannot provide

the port mapping information required for proper routing, the NAT device cannot complete the connection to the host. In this scenario, the following solutions are recommended.

Challenge	Solution
One or more hosts are hidden behind a NAT device.	Adopt a VPN solution combined with Symantec pcAnywhere. <ul style="list-style-type: none">■ The remote user connects to the network using a trusted VPN.■ The remote user then starts pcAnywhere.■ The remote user then connects to the host, either specifying the host IP address or browsing the network for available hosts.
A single host is hidden behind a NAT device.	Configure the NAT table to direct all incoming data from the pcAnywhere ports to that host. The pcAnywhere registered port numbers are 5631 (data) and 5632 (status). These port numbers are configurable. For more information, see the Symantec pcAnywhere online Help.
Multiple hosts are hidden behind a NAT device.	Using pcAnywhere, assign unique port numbers to each pcAnywhere host. Configure the NAT table to direct all incoming data from these pcAnywhere ports to the appropriate host.

Dial-in access

Symantec pcAnywhere supports modem-to-modem connections, which offers another option for resolving the remote access issue. By equipping each client computer with a modem, remote users with modem access can dial in to the host directly. This option can pose a risk because remote users are bypassing any firewall, NAT device, or other security mechanism that is in place on the network.

In the interest of security, many organizations now prohibit or limit the use of modems on client computers that are behind a firewall or other security mechanism. Remote access to network hosts presents a challenge for remote users who dial in via modem. The remote user must first establish a connection with a dial-in server that is attached to the network. Once that connection with an initial host is established, the remote user can then use that connection to connect to other pcAnywhere hosts that are running on the network. This series of connections from one host to another (also known as daisy-chaining) can negatively affect performance. In this scenario, the following solution is recommended.

Challenge	Solution
Dial-in remote users need to connect to one or more network hosts (dial-in, network-out connections)	Adopt a RAS solution combined with Symantec pcAnywhere. <ul style="list-style-type: none">■ The remote user connects to the network using a trusted RAS.■ The remote user then starts pcAnywhere.■ The remote user then connects to the host, either specifying the host IP address or browsing the network for available hosts.

Copyright © 2003 Symantec Corporation.
All rights reserved.

Symantec, the Symantec logo, and pcAnywhere are U.S.
registered trademarks of Symantec Corporation.

Other brands and products are trademarks of their respective
holder/s.