



## Proventia® Desktop Access Control

### Closing the Door on Remote Threats

#### INTERNET SECURITY SYSTEMS' APPROACH TO PROTECTING AGAINST EXTERNAL THREATS FROM REMOTE USERS.

The one area of the network that is notoriously difficult to protect is the same one that could nullify all of your existing safeguards — remote users. Remote user systems are common gateways for network threats. As sales people, business executives and other employees travel or work from home, they can infect their remote system through everyday surfing activities. Once they log in through the virtual private network (VPN), they can transmit malicious code from their remote system into the corporate network.

#### NETWORK ACCESS CONTROL - THE VULNERABILITIES

For many organizations, it is imperative for field employees to have remote access. It is simply unfeasible for remote users to wait until they are physically on site before they are allowed to log into the corporate network. But with this freedom comes risks.

Laptop and remote desktop users frequently access the Internet outside the safe cocoon of the corporate network. Anything the end-user accesses during these sessions may be unregulated by the corporate security precautions set in place.

Wireless hotspots are the fastest growing off-network access method, with more than 13,500 listed hotspots worldwide, according to Wifinder.com. That means there are more than 13,500 potential infection spots for every remote user in your organization if the installed security software isn't active and updated.

#### PROVENTIA® DESKTOP ACCESS CONTROL — INTERNET SECURITY SYSTEMS' INTEGRATED APPROACH TO INFRASTRUCTURE PROTECTION

Proventia Desktop Access Control (PDAC) will insure that remote connections are protected as they connect to the corporate network. It provides organizations with the ability to verify that laptops or desktops connecting to the corporate network are running an updated ISS host protection product.

The access control solution utilizes the following ISS products:

- Proventia Desktop or RealSecure® Desktop
- Proventia Intrusion Prevention Appliance:
  - Proventia G100
  - Proventia G200
  - Proventia G1200 (copper and fiber)
- SiteProtector™ Centralized Management System (SP5 or greater)

## Remote User Security

*73 percent of workers use a laptop as their main computer.*

*86 percent of laptop users inadvertently download software to their laptop.*

*Only 55 percent of companies restrict work laptops to work-related use only.*

*42 percent of laptop users visit peer-to-peer sites and those with adult content using their work-owned laptop.*

*46 percent of workers allow people outside of work to use their laptop, with 22 percent having no idea what purpose it is being used for.*

**Source: Dynamic Markets Ltd.**

## ACCESS CONTROL PROCESS

When a user attempts to connect to the corporate network through the VPN, the VPN Concentrator will verify the user and assign an IP address range. The inline Proventia intrusion prevention appliance will recognize those IP addresses to be originating from the VPN and will send the encrypted traffic to the SiteProtector Agent Manager. Before the traffic can proceed to the rest of the network, the Agent Manager will decrypt the traffic and query the remote user. Based on parameters specified by the administrator, the Agent Manager will verify that the end-user has the proper version of Proventia Desktop or RealSecure desktop installed. If not, the end-user will not be allowed to connect to the corporate network through the VPN ... protecting the internal network from getting inadvertently infected.

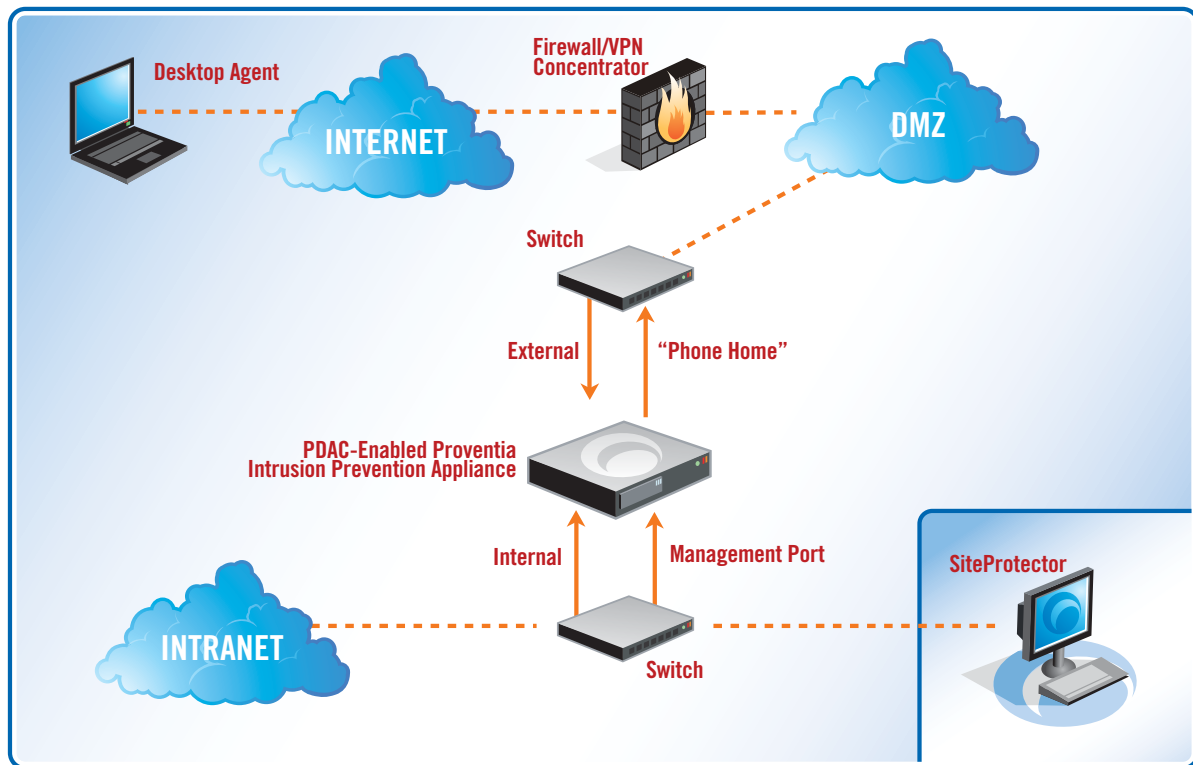


Figure 1: Proventia Desktop Access Control Diagram

Proventia Desktop Access Control is a crucial component of an organization's overall data and systems protection strategy. It reduces the risk associated with remote users logging into the company and spreading viruses, worms, Trojans and other malicious programs, while allowing employees the access they need to remain productive.

Contact us today to learn more about how Proventia Desktop Access Control can help you secure your network and resources. Call 1-800-776-2362 or e-mail [sales@iss.net](mailto:sales@iss.net). Be sure to ask if your company qualifies for a free 30-day trial. For more product information, visit [www.iss.net](http://www.iss.net).

## ABOUT INTERNET SECURITY SYSTEMS (ISS)

Internet Security Systems has long been a trusted security expert for world governments and the Global 500. ISS provides preemptive security products and services that stop Internet threats before impact. Founded in 1994, ISS is publicly traded on the NASDAQ (ISSX) and has its headquarters in Atlanta. ISS protects more than 11,000 global customers, and maintains 1,200 employees operating in 27 countries.

**INTERNET | SECURITY | SYSTEMS®**  
*Ahead of the threat.™*

Copyright© 2005 Internet Security Systems, Inc. All rights reserved worldwide

Internet Security Systems, SiteProtector and Ahead of the Threat are trademarks, and the Internet Security Systems logo, Proventia and RealSecure are registered trademarks, of Internet Security Systems, Inc. All other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

Distribution: General

MC-PDAC- 0705

**NETWORK & HOST INTRUSION PREVENTION | VULNERABILITY MANAGEMENT | MANAGED SECURITY SERVICES**