



F5 White Paper

# F5 FirePass Endpoint Security

Most people perceive remote access as either trusted or un-trusted. But these days, with so many personal devices connecting to the corporate infrastructure, all hosts should be considered hostile until they prove otherwise.

**by Peter Silva**

Technical Marketing Manager



# Contents

<b>Introduction</b>	<b>3</b>
<hr/>	
<b>Challenges</b>	<b>4</b>
Usage Scenarios	5
<hr/>	
<b>Solution</b>	<b>5</b>
Pre-logon Inspection	6
Protected Resources	8
Post Logon	10
<hr/>	
<b>Conclusion</b>	<b>11</b>



## Introduction

As SSL VPN technology has become the standard for organizations extending their internal infrastructures (including cloud deployments) to non-employee users, endpoint security has become a bigger concern. IT acceptance of personal devices and mobile use is increasing, and it is no longer enough to protect your assets from unknown malicious intruders. Organizations also need to protect against employees connecting and entering sensitive user credentials from unpatched personal computers, various mobile devices, or public terminals. The worldwide mobile worker population is set to increase from 919.4 million in 2008 (accounting for 29 percent of the worldwide workforce) to 1.19 billion in 2013 (34.9 percent of the workforce) according to IDC. This is sure to result in more people who will need to have access to the corporate network from mobile devices.

Enterprises and management are facing a potentially tricky business situation. Enabling employee and partner collaboration has become critical as mobile devices have become nearly ubiquitous; but this proliferation of devices has also made workers' locations and work hours more diverse. This means that to keep users productive, organizations must make shared information available to the people that need it, when they need it. To do this, organizations have to provide employees and partners with access to their systems, even during a disaster. A disaster can be a tornado, flood, or hurricane—but it could also be an everyday snowstorm or a child with the flu. If employees can't commute and are snowed in at home, do you declare a snow day and cease operations? What if an employee is sick?

Circumstances like these no longer necessitate a complete halt; working while away from the office is often a viable alternative for users with remote access. But with whom do you share access to your network? Users who access shared files are employees in the office and on the road or at home; but they're also consultants, contractors, partners, and customers using home computers and mobile devices to connect to your network. Between the people and the technology stand the IT staff who must wrestle the sometimes contradictory demands of both management and users, as well as ever expanding and evolving security requirements.

Remote access has become simultaneously easier and more complex. Historically, IPsec has been offered only to employees, with strict settings, specific ports, and virtually no endpoint check, along with a dedicated client. SSL VPN has made it easier for anyone to connect to network resources, but it has also become more complex for the very same reason. With so many different types of users connecting



from various devices to access vastly different internal resources, it is critical to inspect every requesting host to ensure both the user and the device can be trusted.

## Challenges

Because SSL VPN has made remote access available to the masses with nothing more than a browser, you must be able to detect not only the type of computer (laptop, mobile device, kiosk, and so on), but also its overall security posture. With so many Internet-ready devices available, a Windows computer, a Mac or Linux box, and a mobile device could all be trying to gain access at any given moment. It is necessary for the remote access controller to inspect each device before users enter their credentials so you can decide whether you want to allow the connection. If the inspection fails, how should you fix the problem so that the user can have some level of access? If the requesting host is admissible, how do you determine what they are authorized to access? And, if you grant access to a user and their device, what is the guarantee that they neither take nor leave anything proprietary? The key is to make sure that only safe, trusted systems are allowed to access your highly sensitive infrastructure, and that you control what they are allowed to see.

One of the first steps to accomplishing this is to chart usage scenarios. Working in conjunction with the security policy, it is essential to uncover usage scenarios and access modes for the various types of users and devices. The following table is a good example of various usage scenarios.

Usage Scenario	Access Point	Device Owner	Device Security	Enable Downloads?
<b>EMPLOYEE</b>				
Office Worker	LAN	Organization	Managed	Permits
Mobile Worker	Anywhere	Organization	Managed	Permits
Telecommuter	Home	Organization	Managed	Permits
Extended Workday	Home	Third Party	Unmanaged	Permits
Casual Access	Anywhere	Third Party	Unmanaged	Likely Blocks
Teleworker	Anywhere	Employee	Unmanaged	Permits
Shared Computer	LAN	Organization	Managed	Permits



Usage Scenario	Access Point	Device Owner	Device Security	Enable Downloads?
<b>NON-EMPLOYEE</b>				
Office Visitor/ Contractor	LAN	Visitor/Contractor	Unmanaged	Permits
Extranet	Partner LAN	Partner	Shared Responsibility	Permits
Consumer	Anywhere	Consumer	Unmanaged	Permits

## Usage Scenarios

To implement an effective endpoint security policy, an organization must take inventory of possible access situations it is willing to support. Table 1 illustrates options that could be made available for the various access points. The organization must decide how each scenario will be addressed.

Your company's own chart will probably vary based on its Acceptable Use Policy, but this exercise gets administrators started in determining the endpoint plan. The basic flow shows types of users, where they are connecting from, who owns and manages the connecting device (and type of device, if possible), and whether ActiveX or Java downloads are allowed (typically used to run endpoint inspectors). You may also want to include alternate scenarios, for example to accommodate office workers who normally connect to the LAN from a corporate computer, but who now need to access resources from their personal computer on an open WiFi system. While this type of user may be valid, their device is not trusted; therefore you should grant resource access only to a subset of what they normally access by applying more granular controls.

## Solution

Allowing an infected device access onto the network is just as bad as allowing an invalid user to access proprietary internal information. This is where the powerful endpoint security features of F5® FirePass® SSL VPN devices take over. Endpoint security prevents infected PCs, hosts, or users from accessing the system and connecting to the network. Automatic re-routing for infected PCs reduces help desk calls and prevents sensitive data from being snooped by keystroke loggers and malicious programs.



## Pre-logon Inspection

Validating a user is no longer the starting point for determining access; the user's device now gets first review. Pre-logon checks (Figure 1) run prior to the actual logon page appearing, so if the client is not in compliance with the organization's access policy, they will be denied the chance to log on. These checks can determine if antivirus software or a firewall is running and up to date, plus perform many more inspections including OS patch level, machine information, and processes running. FirePass can direct the user to a remediation page for further instructions or even turn on security software automatically for the user. Inspectors can look for certain registry keys or files that are part of your corporate IT build/image to determine whether the device is a corporate asset. Pre-logon checks can retrieve extended Windows and Internet Explorer information to ensure certain patches are in place. If, based on those checks, FirePass finds a non-compliant client but an authorized user, it can create a secure, protected workspace for that session. The user can then enter their sensitive information with a Secure Virtual Keyboard. This can all be done with the easy-to-use FirePass Visual Policy Editor.

The Visual Policy Editor is a simple flowchart-style GUI, which makes complex policy creation and enforcement simple and flexible. Using the Visual Policy Editor, you can create a pre-logon security policy that evaluates each endpoint system looking to access the FirePass-controlled network. FirePass provides various pre-built policy templates that cover areas like antivirus/firewall, Google desktop, and client certificates to help automate initial policies. You can also completely custom-build policies using a blank template. All an administrator needs to do is point and click to build the rules and, based on the result, determine what action to take.

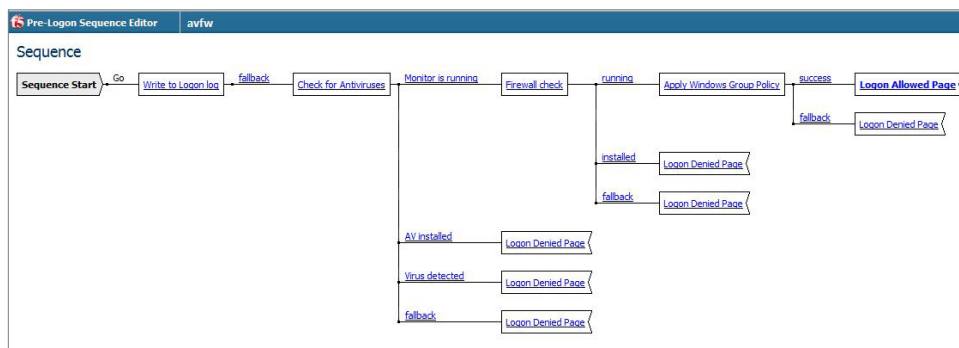


Figure 1: FirePass pre-logon checks

FirePass version 7.0 fully integrates with FullArmor's GPNywhere. This means that you can now provide endpoint security checking and session-based policy



enforcement to any endpoint client requesting access to corporate resources—whether the client is part of a Microsoft Active Directory domain or not. This benefits customers by extending Windows Group Policy enforcement—without the domain access limitations of Active Directory. It also helps companies maintain complete compliance as standards change, and it provides active enforcement with centralized management to prevent policy decay. Integrated endpoint security is built in to FirePass, but it can also be used with third-party endpoint inspectors such as WholeSecurity’s Confidence Online Server.

For more information about Group Policy, read the “[Get to Know GPO](#)” white paper.

After a user types in their company’s unique FirePass URL address, they get visual indication of the inspection as it gathers information about the user’s system. The pre-logout sequence (Figure 2) determines which inspectors to activate depending on the evaluation.

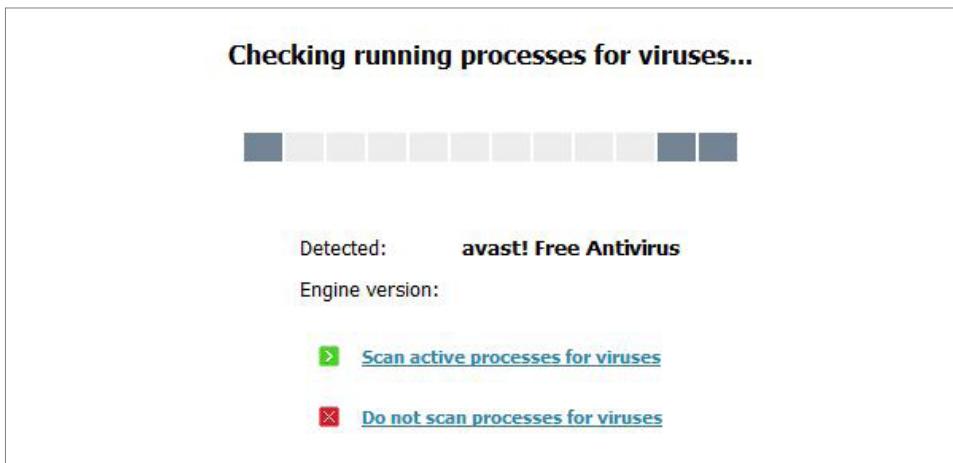
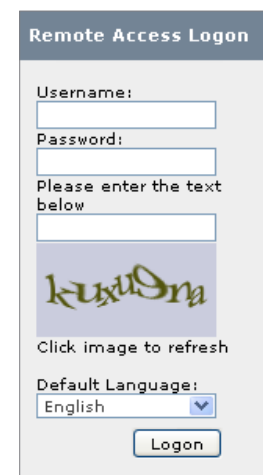


Figure 2: FirePass pre-logout sequence

Ideally, the device passes and the user is directed to the logon page. However, if logon is denied, it is easy to educate the user as to why the failure occurred and relay steps to resolve the problem. For example, the user may receive this message: “We noticed you have antivirus software installed but not running. Please enable your antivirus software for access.” In certain deny instances, rather than denying logon and communicating a detailed remedy, FirePass can immediately re-direct the client to a remediation server designed to correct or update the client’s software environment, ensuring policies required for a pre-logout check are satisfied without any user interaction. Pre-logout inspection is an important first step in endpoint security because it enables administrators to assess the requesting device before granting logon. Once the user makes it to the logon page, FirePass offers CAPTCHA support to help prevent possible script-based brute force attacks on users’ passwords.





If administrators are still unsure about the device or want to allow controlled access, they can use Protected Workspace (PWS). With PWS, you can restrict users from printing, saving files, or storing information on a client accessing your network or system via FirePass. It restricts users to a temporary, virtualized workspace and file system on the remote device, which contains temporary Desktop and My Documents folders. In protected mode, the user cannot intentionally or accidentally write files to locations outside the temporary folders. The files that are accessed are encrypted so if PWS doesn't close normally (for example, in the event of a power failure), the remnants of that content are virtually unreadable. The PWS control deletes the temporary workspace and all of the folder contents at the end of the session. PWS is especially beneficial to financial, healthcare, and government entities that regularly access sensitive information. It is also useful when people are working on devices that aren't controlled by IT and should not store any information.

## Protected Resources

Ultimately, as the ever-expanding virtual network grows, internal corporate resources require the most protection. Most organizations don't necessarily want all users' devices to have access to all resources all the time. Working in conjunction with the pre-logout sequence, FirePass uses a protected configuration to gather device information (like IP address or time of day) and measure risk factors to determine whether a resource favorite should be offered. FirePass can create detailed protected configurations using a variety of security measures. It can check whether a logon is coming from a trusted network, what antivirus software the endpoint is running, and which certificate the client is using. The many different checks cover protection criteria (Figure 3) such as loggers, virus infections, information leaks, and unauthorized access. Administrators can then select the safety feature needed to negate each risk factor.

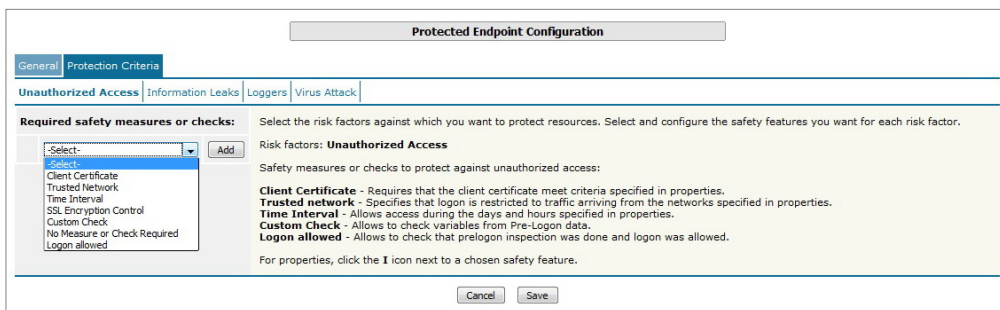


Figure 3: Protection criteria



For example, Sample Company, Inc. (SCI) has some contractors who need network access to its corporate LAN. While this is not an issue during work hours, SCI does not want them accessing the network after business hours. With the proper configuration, FirePass can check the time when a contractor tries to log on at 10 p.m.; FirePass already knows the contractor network access favorite is only available during SCI’s regular business hours, which are 9 a.m.–5 p.m.

Because of this, the network access link the contractor normally sees during regular business hours will vanish during non-business hours. If the user’s endpoint protection does not satisfy the defined level, the system disables access to resources.

Protect Resources		
Resource		Required protection
Firepass Webtop		Select
Web Application Tunnels		Select
Network Access		Select
Connection in binkyrg1	time	
Connection in binkyrg2		
Connection in Endy_test		
Connection in F5Resources		Select
Connection in psilva		
Connection in sdrack		
Connection in ssa_resource		
AppTunnels		Select
Legacy Hosts		Select
Terminal Servers		Select
Web Applications		Select
Windows Files		Select
Resource group		Required protection
Accounting		Select
binkyrg1	Windows	Select
binkyrg2	Non-Windows	Select
Default_resource		Select
Endy_test		Select
F5Resources		Select
HR		Select

Figure 4: Endpoint security—protect resources

SCI may still enable access to certain web applications, such as an extranet portal, after hours, but not to a full SSL VPN tunnel. The potential access scenarios are endless, but FirePass endpoint security makes designing the configurations seem elementary. After determining, via pre-logout inspection, that the device is safe, the next step is to protect your resources.



## Post Logon

Post-logon actions can protect against users leaving sensitive information on the client. FirePass can impose a cache-cleaner to eliminate any user residue such as browser history, forms, cookies, auto-complete information, dial-up entries, and more. FirePass can also close Google desktop search so nothing is indexed during the session. For systems on which you are unable to install a cleanup control, you can configure FirePass to block all file downloads to avoid temporary files being inadvertently left behind—yet still allow access to the applications users need. Post-logon actions are especially important when you allow non-trusted machines access, but you don't want them to take any data with them after the session.

### Post-Logon Actions

- Inject ActiveX/Plugin to clean-up client browser web cache.
  - Require cache cleanup ActiveX/Plugin to be loaded to allow attachment downloads in Mobile E-Mail and downloads via Web Applications.
  - Require cache cleanup ActiveX/Plugin to be loaded to allow file downloads in Windows Files. If not loaded - only download of Zip archives allowed.
  - Force FirePass 4100 session termination if the browser or Webtop is closed.
  - Uninstall FirePass 4100 client components.
  - Remove dial-up entries used by Network Access client.
  - Uninstall ActiveX components downloaded during FirePass 4100 session.
  - Empty Recycle Bin.
- Clean forms and passwords autocomplete data.
- Close Google Desktop Search.
- Inherit caching policy settings from Portal Access Web Applications configuration. [Click here to view Portal Access configuration.](#)

Terminate users' sessions when they are inactive  
is Disabled ▼

Lock users' lockstations when they are inactive is Disabled ▼

update

Figure 5: Post-logon actions

In summary: first, inspect the requesting device. Second, protect resources based on the data gathered during the check. Third, make sure no session residue is left behind.

## Conclusion

Security is a question of trust. Is there sufficient trust to allow a particular user and a particular device full access to enterprise resources? Today, all clients are a risk, and endpoint security gives the enterprise the ability to verify how much to trust the user and device, and to determine whether to grant the client access to all, some, or none of its resources. FirePass integrated endpoint security provides:

- Automatic detection of security-compliant systems to prevent infection.
- Automatic integration with the most virus scanning and personal firewall solutions in the industry (more than 100 different antivirus and personal firewall versions).
- Automatic protection from infected file uploads or email attachments.
- Automatic re-routing and quarantine of infected or non-compliant systems to a self-remediation network to reduce help desk calls.
- Secure workspace to prevent eavesdropping and theft of sensitive data.
- Secure logon with a randomized key entry system to prevent keystroke logger snooping.
- Full integration with the FirePass Visual Policy Editor. This enables you to create custom template policies based on the endpoints accessing the network and the company's security profile.

**F5 Networks, Inc.** 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 [www.f5.com](http://www.f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)

