Get to Know GPO

This paper covers the F5 FirePass integration with FullArmor's GPAnywhere. FullArmor is a leading provider of enterprise policy management on the Microsoft Windows platform. Also, in this paper, we'll get to know Group Policy Objects.

White Paper

by Peter Silva

Introduction

With the explosive growth of road warriors, telecommuters, temporary workers, and mobile users, it is virtually impossible for organizations to ensure that endpoint devices remain secure and compliant. Even devices that initially are fully compliant may become non-compliant when settings are inadvertently changed or when new corporate policies are implemented. IT administrators must be able to enforce consistent, current policy settings on endpoints whether they are connected or disconnected from the enterprise's Active Directory domain. This paper covers the F5 FirePass integration with FullArmor's GPAnywhere. FullArmor is a leading provider of enterprise policy management on the Microsoft Windows platform. Also, in this paper, we'll get to know Group Policy Objects (GPO).

Flexibility and simplicity is vital for enterprises struggling to manage and secure the numerous access policies of their mobile workforce. Policies cannot be applied with a “one size fits all” approach. Some organizations divide users into location or connection type categories like corporate office, home office, wireless, mobile, kiosk, and so forth. It really comes down to a determination of whether the device is trusted—such as a corporate laptop—or whether it is untrusted device— like a home computer. The potential risks of these devices are different so they must be treated as such. Traditionally, Group Policies for remote clients have been dependent on centralized Active Directory (AD) domain controller services and have been limited to the network domain boundaries defined by AD security and administration. This means a device had to be both part of and connected to the domain for a policy to be enforced, since it must be pushed to the device. Active Directory and Group Policy go hand in hand. However, there are limitations that are outside this influence, such as remote and non-AD endpoints that need policy enforcement and remediation when they connect to an organization's intranet.

Endpoint lockdown and security is a continuously moving target. Most major legislation requires security auditing for any device that connects to the infrastructure. Financial institutions are also imposing more strict auditing legislation and verification for end-to-end financial transactions.

Session-Based Policy Enforcement

In a policy-based environment, data traffic can travel different routes based on the user's session characteristics. The Policy Enforcement Point makes the device aware of specific services and resources that are available for the duration of the session.

What Happens

For example, Barry wants to connect to the corporate VPN network from his home machine through his company's FirePass SSL VPN appliance. Corporate IT has mandated a set of security policies that must be in place during a VPN session to ensure compliance and security. The policy might include, but is not limited to, disabling the USB drive, restricting CD-ROM access, or disabling changes to the control panel. This policy is in place because Barry is using his home computer and corporate IT does not trust it. The policy might also state that the device has antivirus/firewall software running, or that the user only has access to certain resources. Barry opens his browser and types in his SSL VPN location. His company's FirePass device is configured to initiate an endpoint host security check before access is granted. Before the connection is allowed, an IT mandated policy is automatically downloaded (via browser control) and applied to Barry's machine. If Barry was using his trusted corporate laptop, some or all of the restrictions might not be required. Active Directory administrators have control of more than 2800 different settings to ensure the proper policy is being applied to the proper endpoint.

How it Happens

When the FirePass device is about to grant the connection, a FirePass browser-based control downloads a GPAnywhere template that has been assigned to Barry's PC by the administrator. The agent then executes a local GPAnywhere utility to check digital signatures, back up the current user's policy environment, and execute the downloaded Group Policy template to the PC. Upon disconnect, the browser-based agent calls the GPAnywhere utility to undo the policy and restore the PC's original configuration. So, when Barry ends his FirePass session, his computer is returned to the state it was in before the connection.

The integration of Group Policy with FirePass provides enhanced, strong endpoint security lock-down for client devices that mitigates the potential for security breaches. This is especially relevant because of the many regulatory laws governing data security. FirePass v6.03 comes with specific templates for particular regulatory compliance. This new FirePass feature equips enterprises with a choice of templates to suit their specific policy requirements, which is especially critical for evolving corporate governance and compliance mandates such as PCI, HIPPA, and GLBA. You can find more information about this in the FirePass Implementation section.

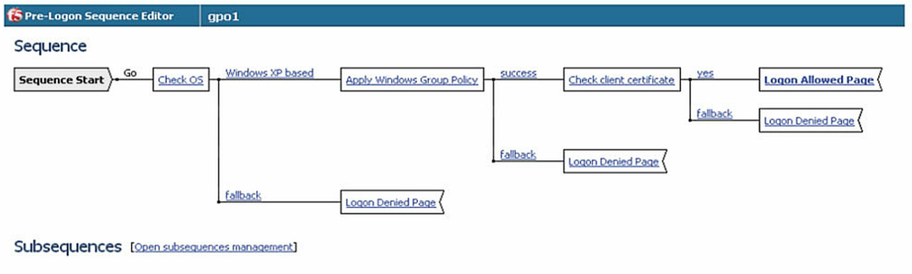

Figure 1: Visual Policy Editor example

FirePass Integration

Cleanly integrating all of the available Group Policy settings and features, FirePass delivers standard-based policy management to secure and configure the endpoint along with ensuring up-to-date enforcement is applied and monitored. With this integration, you can enforce and remediate to any endpoint requesting secure access to applications through the delivery of Group Policy.

Connection-Based Policy Application

The GPAnywhere Inspector is configured in the FirePass Visual Policy Editor; the client might also be invoked by FirePass before a user logs in to ensure endpoint integrity.

Upon a request for connection, the appropriately downloaded or available Group Policy template file is executed through a call to the GPAnywhere utility, which has elevated access to local administrator level through the FirePass client software. After the GPAnywhere utility is called, it signifies the type of action to be taken and the location of the Group Policy template to be enforced. After the session is disconnected, the previously backed-up policy state of the machine is restored. The settings are then back to normal.

The Group Policy settings are spoken language-neutral because they control the device's hardware/software configuration regardless of language. For custom configurations using the GPAnywhere console with Active Directory, a language-appropriate version is available.

The spoofing of a Group Policy template poses a major security threat and thus, the subsequent execution of a non-authorized EXE with an elevated privilege. To mitigate this threat, the GPAnywhere utility—responsible for policy execution—is elevated via the GPAnywhere driver. Both the GPAnywhere driver and utility are both signed and securely installed, and accept signed Group Policy template files for execution. With Policy Template Signature Verification, the client executable will only apply a template that is signed with the FullArmor or F5 Authenticode certificates.

Policy Rollback

Two strategies can be used to address the case when the FirePass session does not close as planned. The GPAnywhere utility will create shortcuts on all users' desktops, and in all users' start menus, to rollback (restore) policies applied by the FirePass session. Or, the utility can create registry entries to trigger a rollback during the next system boot. When rollback is triggered, all shortcuts and registry entries will be removed.

FirePass Implementation

Note: To use the Microsoft Windows Group Policy Inspector with a pre-logon sequence, you must install the Group Policy license on the controller, which can be obtained from your F5 sales representative or reseller. To create custom Group Policy templates, you must purchase GPAnywhere from FullArmor. For information on the templates and step-by-step instructions on how to configure FirePass with Group Policy, please contact Online Help directly from your device or visit AskF5 at https://support.f5.com/kb/en-us/solutions/public/9000/100/sol9157.html. Out of the box, the FirePass 6.0.3 device with Group Policy module comes with nine pre-loaded templates covering various areas of use.

Predefined Group Policy Templates

Name	Description
EC Domain Template XPSP2 Desktops (User).exe	Microsoft Enterprise Client Policy for desktops and laptops. This is a moderate policy, balancing security and usability.
SSLF Domain Template.exe	Microsoft Specialized Security (Limited Functionality) for desktops and laptops. This is a more focused security policy, with greater restrictions on configuration access.
Lightly Managed Template.exe	Microsoft Common Usage (light) for desktops and laptops. This policy is used in managed environments, and provides light restrictions on user access to devices, configuration, and applications.
Highly Managed Template (User).exe	Microsoft Common Usage (high) for desktops and laptops. This policy is used in managed environments and provides high restrictions on user access to devices, configuration, and applications.
Terminal Services Task Station Template.exe	Terminal Services for client terminal services. This policy is used in environments where the primary use is terminal services.
Firewall Settings Template.exe	FirePass settings for enabling the user's firewall. This policy is used to ensure the user's Microsoft firewall is configured and running.
GLBA Template.exe	Based on the GLBA standard. This policy is used for desktop and laptops to help prevent access to unauthorized information.
HIPAA Template.exe	Based on the HIPPA standard. This policy is used for desktop and laptops to help prevent access to unauthorized information.
PCI Template.exe	Based on the PCI standard. This policy is used for desktop and laptops to help prevent access to unauthorized information.

Table 1: Predefined Group Policy templates

EC and SSLF

The EC and SSLF templates are based on Microsoft security profiles for Enterprise Client (EC) and Specialized Security—Limited Functionality (SSLF) environments. Microsoft uses the EC and SSLF environment classifications as the basis for making recommendations on how to configure a variety of server, workstation, and laptop settings.

The EC Domain Template is applicable to the majority of enterprise environments. It balances security with usability concerns. The Group Policy settings suggested for users in EC Domain-classified environments focus on addressing the basics at a moderate level, so it is not intrusive to the user.

Examples of settings that are applied as part of the EC Domain Template are:

- Disabling Internet Explorer's automatic saving of passwords.
- Requiring the user to reenter their password after a system suspend.

The SSLF Domain Template is applicable to environments where concerns about security are paramount. In such an environment, some usability is sacrificed in order to further secure the systems. The Group Policy settings suggested for users in SSLF Domain-classified environments expand upon the settings recommended for the EC Domain.

Examples of settings that are applied as part of the SSLF Domain Template are:

- Disabling user access to the IE Security settings.
- Disabling user access to system tools such as the registry editor.

Additional information can be found in the Windows Server 2003 security at www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch01.mspx. guide.

Microsoft Common Scenarios

The highly and lightly managed templates are based on Microsoft Common Scenarios. The Common Scenarios classify client machines into categories such as mobile, multi-user, app-station, task-station, or kiosk. To standardize the implementation of the scenarios, Microsoft defined the highly-managed and lightly-managed Group Policy settings as the base set of settings on top of which the scenarios would be implemented.

Both the lightly-managed and highly-managed policies are intended for use with devices that work in a centrally managed environment. As such, both templates restrict what configuration options a user has access to. The distinction between the two is a matter of degree.

In the case of the lightly-managed template, the user retains some ability to customize their desktop environment. Examples of settings that are applied as part of the lightly-managed template are:

- Enabling user access only to the Desktop Control Panel applet.
- Prohibiting access to the Add/Remove Programs Windows Components page.

In the case of the highly-managed template, the user is given very little leeway to customize the desktop environment. Examples of settings that are applied as part of the highly-managed template are:

- Prohibiting access to the Control Panel.
- Denying access to Add/Remove Programs.
- Prohibiting Adding Printers.

For additional information, read Implementing Common Desktop Management Scenarios at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/csws2003.mspx?i=4255.

The Terminal Services Task Station Template is specific to Terminal Server users. It prevents users from reverting back to the default security policy but more importantly, it controls which file types (.exe, .bat, .msi) can be used. While there are no restrictions on shortcuts (.lnk), restrictions are placed on actual path of executables.

The Firewall Settings Template does exactly what it says—enables user's firewall. This policy is used to ensure the user's Microsoft firewall is configured and running. If the Microsoft Windows Firewall is not enabled, Group Policy will turn it on.

The final three pre-configured templates help address certain regulatory requirements. They are all based on a basic security policy with their own nuances.

GLBA

GLBA (Gramm-Leach-Bliley Act), also known as the Financial Services Modernization Act, enabled investment banks to merge with commercial banks and permitted insurance services to merge with securities companies. Another important part of the Act deals with privacy and the policies in place to protect that sensitive information from security threats and ensures the integrity of the data. These cover the collection, disclosure, and protection of an individual's non-public, personally identifiable information. With GLBA, financial institutions must now inform the consumer, through a privacy notice, how the company collects, stores, shares, and safeguards the data. GLBA is mandatory for any financial services company.

Examples of settings that are applied as part of the GLBA template:

- Disabling CD-ROM and floppy drive access.
- Digitally signing all communications, if available.
- Prohibiting the user from modifying any certificate settings.
- Prohibiting access to the Advanced Settings menu in Network Connections.

HIPPA

HIPAA (Health Insurance Portability and Accountability Act) not only protected people with continued health insurance coverage if they lost or changed jobs but also established guidelines for the exchange of patient data, including electronic transmission. There are privacy rules for the use and disclosure of Protected Health Information (PHI) both paper and electronic, which are things like current health status, personal physician, and any part of a person's medical record— including diagnosis or treatment—or payment history are covered. HIPAA states that this information must be protected.

Examples of settings that are applied as part of the HIPAA template:

- Restricting CD-ROM access to locally logged-on users only.
- Prohibiting access to the Advanced Settings menu in Network Connections.
- Locking workstation if smartcard is removed.
- Clearing virtual memory.

PCI DS

PCI DSS (Payment Card Industry Data Security Standard) was designed by the major credit card companies as a guideline for organizations that process credit card transactions. Like GLBA and HIPAA, it establishes procedures for processing, storing, and transmitting of sensitive data along with protecting against security vulnerabilities/threats, which may expose that information. Companies must also go through an outside audit to validate their compliance. There are 12 requirements within 6 major areas of concern: network security including Monitoring and Testing, Protecting Cardholder data, Vulnerability Management, Access Control, and Policy Maintenance. You can find the specifics of PCI DSS at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Examples of settings that are applied as part of the PCI template:

- Suspend session after 15 minutes of inactivity.
- Restrict anonymous access to Named Shares.
- Disable Advanced Settings in Internet Explorer.

Custom Policy Templates

In addition to the policy templates available in FirePass out-of-the-box it is possible to develop and deploy custom policy templates to VPN clients. Custom Policy Templates, while not included in the base Group Policy package, are an important feature, and give the administrator the ability to create specific templates based on their own criteria.

The policy templates are based on and derived from GPOs. They are generated using the GPAnywhere for VPN Console, available from FullArmor. More information can be found at FullArmor's website (http://www.fullarmor.com).

Conclusion

Through the FirePass integration of FullArmor GPAnywhere, it is now possible to provide endpoint security checking and session-based policy enforcement to any endpoint client connecting to FirePass—whether they are part of an AD domain or not. This new feature benefits customers by:

- Extending Group Policy enforcement —without the domain access limitations of Microsoft Active Directory (AD).
- Enhancing endpoint security to mobile workers and non-trusted devices.
- Ensuring simple and quick implementation, with ready-to-use policy templates.
- Preventing breaches with secure endpoint protection.
- Maintaining complete compliance as standards change.
- Providing active enforcement with centralized management to prevent policy decay.

GPAnywhere Utility: A FullArmor tool signed and installed via FirePass that will check digital signatures and is called by the FirePass agent to execute Group Policy templates.

GPAnywhere Driver: A FullArmor tool signed and installed via FirePass that will elevate the GPAnywhere utility to local administrative access right while running under the current user context

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com