WSA - HW – 8 :

4. Describe the commond differences between AppLocker and Software Restriction features.

Software Restriction Policies (SRP) was originally designed in Windows XP and Windows Server 2003 to help IT professionals limit the number of applications that would require administrator access. With the introduction of User Account Control (UAC) and the emphasis of standard user accounts in Windows Vista, fewer applications today require administrator privileges. As a result, AppLocker was introduced to expand the original goals of SRP by allowing IT administrators to create a comprehensive list of applications that should be allowed to run.

The following table compares AppLocker to SRP:

Feature	Software Rest. Policies	AppLocker
Rule scope	Specific user or group (per GPO)	Specific user or group (per rule)
Rule conditions provided	File hash, path, certificate, registry path, and Internet zone roles	File hash, path, and publisher rules
Rule types provided	Allow and deny	Deny
Default rule action	Allow and deny	Deny
Audit-only mode	No	Yes
Wizard to create multiple rules at one time	No	Yes
Policy import or export	No	Yes
Rule Collection	No	Yes
PowerShell Support	No	Yes
Custom error messages	No	Yes

Blacklisting and Whitelisting

Malware-protection programs such as antivirus and antispyware software often use a technique referred to as blacklisting to protect computers. Programs that employ blacklisting allow everything to be stored on a computer other than files that are infected with threats listed on the blacklist. If a file is infected, these programs will either delete or quarantine it. An emerging approach to combating malware is whitelisting. Whitelisting takes an opposite approach to blacklisting - that is, the protection program blocks everything except the files that are on its whitelist.

When it comes to protecting computers against the execution of unwanted malware, whitelisting is preferable to blacklisting. Whitelisting eases the life of the administrator, because in today’s interconnected world, users are typically allowed to run fewer applications than they should be blocked from running - including an almost unlimited number of unknown malicious executables that users might download from the Internet. However, whitelisting creates the risk of locking yourself out if you don’t use it properly. For example, you might neglect to add your management applications to the whitelist. In addition, you can

inadvertently prevent your users from working if you forget to add one of their applications to the whitelist.

SRPs and AppLocker both support whitelisting and blacklisting, although they have different default policies. AppLocker uses whitelisting by default, thereby blocking everything; the administrator must explicitly define the applications that can run. The default SRP configuration uses blacklisting, which allows all applications to run; the administrator must define exceptions for any applications to be blocked. Setting up whitelisting with SRPs is difficult, which is why most admins use it only for blacklisting applications. AppLocker is much better suited to provide whitelisting-based protection for controlling applications.

Setting Up AppLocker Rules

To begin, you must know how to configure application restriction rules in AppLocker. As with SRPs, you can use Group Policy Object (GPO) settings to configure and enforce AppLocker rules. You can also use PowerShell cmdlets to configure AppLocker rules (this option isn't available for SRPs). For information about using PowerShell cmdlets with AppLocker, see the MSDN Windows PowerShell Blog entry http://blogs.msdn.com/b/powershell/archive/2009/06/02/getting-started-with-applocker-management-using-powershell.aspx

Create Default Rules.

The preferred option for getting started with AppLocker rule definitions is Create Default Rules. Default rules are generated automatically; these rules are tailored to let Windows run and to let you do your administrative work—both of which are important, considering AppLocker's default whitelisting approach and the risk of locking yourself out. As a safety net, AppLocker prompts you to automatically create the default rules if you try to create a new rule and haven't yet created the default rules.

AppLocker's default rules are relatively open. For example, they include a rule that gives members of the local administrators group access to all local files. An AppLocker best practice is to first create default rules, then refine them using more restrictive rules that you create manually through the Create New Rule option (which I explain later). Default rules can be created separately for each of the three rule types: Executable Rules, Windows Installer

Rules, and Script Rules.

Automatically Generate Rules. With the Automatically Generate Rules option, AppLocker basically generates a whitelist for you. Based on the file folder you provide in the automatic rule generation wizard, AppLocker will propose a set of rules for the files in that particular folder. This important new AppLocker feature isn't included in SRPs. With SRPs you must define the whitelist yourself. To automatically generate a rule set, select Automatically Generate Rules from the Executable Rules, Windows Installer Rules, or Script Rules context menu. On the wizard's first screen, select a file system location on the reference machine, indicate the users or groups you want the whitelist to apply to (an important option that isn't available in SRPs), and provide a name for the resulting rule set.
Note that AppLocker doesn't offer the network zone (aka Internet zone) file identification option that SRPs provide, which lets you use the Internet zone of the website from which code was downloaded to identify the code.

Enforcing AppLocker Rules

Like SRPs, AppLocker isn't enabled by default. Even when you're done creating rules, AppLocker won't immediately enforce them on your clients. Rule enforcement requires two additional steps. First, you must specify whether you want to enforce your rules or run them only for auditing purposes. Second, you must ensure that the Application Identity Service is running on the targeted machines.

The Audit only option is a useful new feature that isn't available with SRPs. When a rule collection is set to Audit only mode, the rules within that rule collection aren't enforced, but any time a user runs an application that's affected by a rule, information about the rule and the application write to the local machine's AppLocker event log container.
Note that the Advanced tab of the AppLocker container's properties refers to a fourth AppLocker rule collection:
DLLs, to cover the *.dll and *.ocx file formats. Microsoft set this rule collection apart in the Advanced tab because of the performance impact DLL checking has when it's enabled. In addition, the process of whitelisting all the allowed DLLs creates a significant amount of administrative overhead. You should enable AppLocker DLL protection only in organizations with extremely critical IT security (e.g., government or defense organizations).

The last step in guaranteeing AppLocker enforcement is to make sure the Application Identity Service is enabled on your Server 2008 R2 and Windows 7 machines. This service is set to manual startup by default. To properly use AppLocker, you must set the service to start up automatically. You can use GPO settings to configure all your machines at once. Because anyone with local administrator rights can stop the service and therefore bypass AppLocker policy enforcement, you need to keep tight control over your administrator accounts.

A Major Step Forward

Like SRPs, AppLocker requires regular rule updates to properly deal with patches and new versions of protected applications. AppLocker can't yet deal with software updates in a dynamic and silent fashion. For this purpose, certain third-party whitelisting applications (e.g., Coretrace's Bouncer, Bit9's Parity) will perform better. In addition, these applications provide broader platform and file-type support. However, AppLocker is a major step forward for application whitelisting in Server 2008 R2 and Windows 7, compared with SRP blacklisting. Windows administrators will appreciate AppLocker's ability to automatically create whitelists, to run in audit-only mode, and to limit rule application based on user and group accounts

Sources:
http://technet.microsoft.com/en-us/library/dd723678%28v=ws.10%29.aspx

http://technet.microsoft.com/en-us/library/ee619725%28v=WS.10%29.aspx#BKMK_SRPdifferences

http://kurtsh.com/2012/03/23/info-difference-between-software-restriction-policies-windows-7s-applocker/

http://windowsitpro.com/security/applocker-windows-server-2008-r2-and-windows-7