F5 FirePass Endpoint Security

Overview

As SSL VPN technology becomes more mainstream and organizations extend their internal infrastructures to users who are not necessarily employees, Endpoint security has become an increasing concern. It is no longer enough to protect your assets from an unknown malicious intruder. Organizations need to protect against trusted employees connecting from their un-patched home computers or protect against that same trusted employee entering their sensitive user credentials on a public terminal at a conference.

Remote Access has become simultaneously easier and more complex. IPSec typically has only been offered to employees, with strict settings, specific ports and virtually no endpoint check. SSL VPN has made it easier for anyone to connect to network resources while becoming complex for the very same reason. With so many different types of users connecting from a slew of various devices, and needing access to vastly different internal resources, it's important to inspect every requesting host to ensure both the user AND the device can be trusted.

Challenges

Since SSL VPN has opened remote access to the masses, and all that's required for this access is a browser, you must be able to detect not only the type of computer (Laptop, PDA, kiosk, etc.) but also its security posture. With so many Internet ready devices available, at any given moment there could be a Windows computer, a Linux box and a WAP phone all trying to gain access. Inspecting each of these to make sure it's something you want to allow before users enter their credentials is a necessity. If the inspection fails, how should the problem be fixed 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 a user and their device are allowed, what is the guarantee that nothing proprietary either gets taken or left behind? The key challenge is to make certain only a 'safe' system is allowed to access your highly sensitive infrastructure.

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 the usage scenarios and access modes for both the various types of users along with the multitude of devices that they may be using. The following table gives a good example of various usage scenarios.

Usage Scenarios

In the course of implementing an effective endpoint security policy an organization must take inventory of the possible "access modes" it is willing to support. The table below illustrate the universe of access's options that could be made available. The organization must decide proactively how each scenario will be addressed.

Usage Scenario	Access Point	Device Owner	Device Security	Allows Downloads?
EMPLOYEE				
Office Worker	LAN	Organization	Managed-Trusted	Permits
Mobile Worker	Anywhere	Organization	Managed-Trusted	Permits
Telecommuter	Home	Organization	Managed-Trusted	Permits
Extended Workday	Home	Employee	Unmanaged-Untrusted	Permits
Casual Access	Anywhere	3rd Party	Unmanaged-Untrusted	Likely Blocks
	Anywhere	Employee	Unmanaged-Untrusted	Permits
Shared Computer	LAN	Organization	Managed-Trusted	Permits
NON-EMPLOYEE				
Office Visitor/Contractor	LAN	Visitor/Contractor	Unmanaged-Untrusted	Permits
Extranet	Partner LAN	Partner	Shared Responsibility	Permits
Consumer	Anywhere	Consumer	Unmanaged-Untrusted	Permits

Note: Access point could be wired or wireless

Source: SSL VPN Central

The resultant chart will probably vary, 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 that device (and type of device, if possible) and if ActiveX or Java downloads are allowed (typically used to run endpoint inspectors). There could even be alternate scenarios since there may be times when “Office Worker”, who normally connects to the LAN from a corporate computer, needs to access resources coming from their personal computer on an open Wi-Fi system. It is important to instantly recognize that while this may be a valid user, their device is not trusted, and thus you should only grant access to a subset of what they normally get by applying more granular access 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 F5’s FirePass’ powerful Endpoint Security features take over. Endpoint Security prevents infected PCs, hosts, or users from 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.

Prelogon inspection

Validating a user is no longer the starting point for determining access; the device that they’re using now gets first review.

Prelogon checks (figure 1) run prior to the actual logon page appearing, so if the client is not in compliance, they won’t even get the chance to logon. These checks can determine if antivirus or firewall is running and if it is up-to-date, along with many more inspectors.

FirePass can direct the user to a remediation page for further instructions or even turn on antivirus or firewall for the user. Inspectors can look for certain registry keys or files that are part of your corporate computer build/image to determine if this is a corporate asset. Prelogon can retrieve extended Windows and IE info 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 and have the user enter their sensitive information with a ***Secure Virtual Keyboard***. This can all be done with the product's easy-to-use ***Visual Policy Editor***.

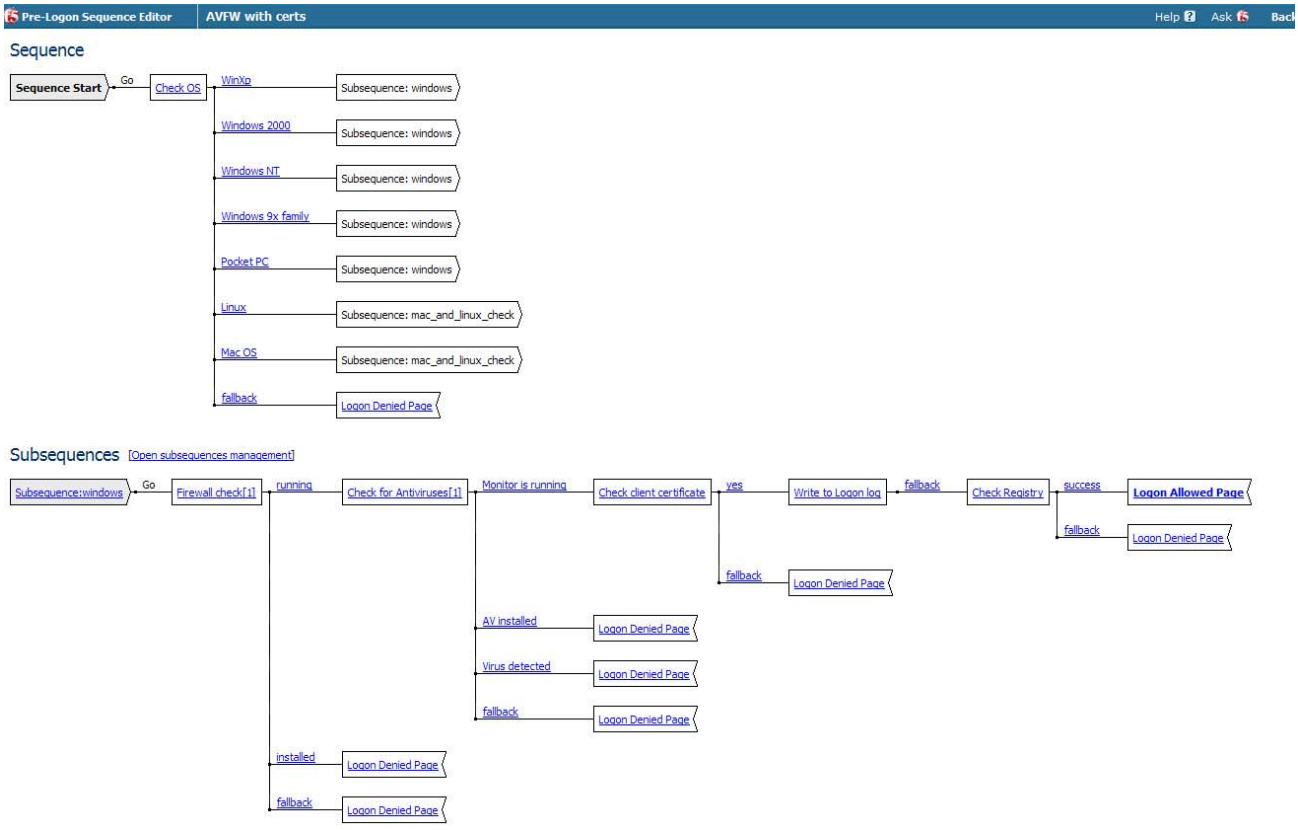


Figure 1: *FirePass Prelogon checks*

The Visual Policy Editor is a simple GUI which makes complex enforcement simple and flexible. Using the Visual Policy Editor, it is possible to create a prelogon security policy which evaluates each endpoint system looking to logon to the FirePass controlled network. FirePass provides various pre-built templates, including over 25 different antivirus/firewall vendors, and Google desktop and client certificates to help automate initial policies. It also allows you to start with a blank template to allow complete custom-built policies. All an administrator needs to do is "point and click" to build the rules and, based on the result, the action to take. FirePass integrated Endpoint Security is built-in, but can also be used with 3rd party end-point inspectors such as WholeSecurity's Confidence Online™ Server.

For the user, after typing in the secure FirePass address, they get visual indication of the inspection as it gathers information about the end user's system. The prelogon sequence (Figure 2) determines which inspectors to activate depending on the evaluation.

Figure 2: *FirePass prelogon sequence*

Hopefully, the outcome is a success and the user gets their logon page. The second outcome, of course, is *logon denied*. It's common to educate the user as to why the failure occurred and possible steps to resolve the problem: '*We noticed you have antivirus installed but not running. Please enable your anti virus software for access*.' In certain deny instances, FirePass could immediately re-direct the client to a remediation server. Rather than deny logon with details, you can automatically send them to a remediation website designed to correct or update the client's software environment, assuring policies required for a pre-logon check are satisfied without any user interaction.

If administrators are still unsure about the device or want to allow controlled access, then Protected Workspace is available. ***Protected Workspace*** (PWS) allows you to restrict end users from printing, saving files, or storing information on a client accessing FirePass. It restricts users to a temporary workspace on the remote system, which contains temporary Desktop and My Documents folders. In protected mode, the user cannot unintentionally or accidentally write files to locations outside the temporary folders. The PWS control deletes the temporary workspace and all of the folder contents at the end of the session. Protected Workspace is especially useful when users are working on devices that should not store information, such as thumb drive, that is not controlled by IT.

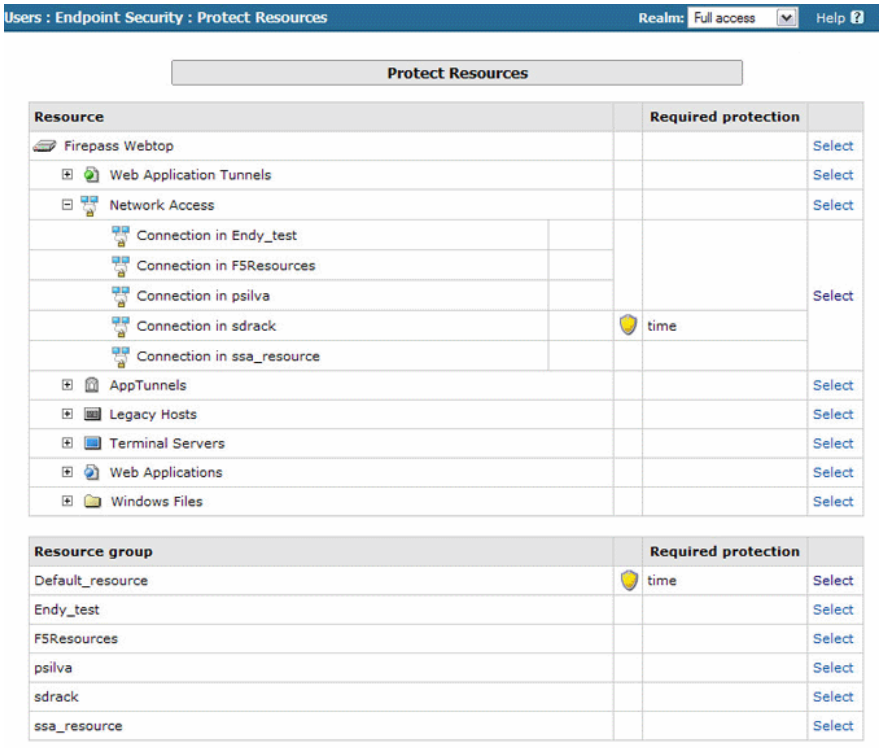
Prelogon inspection is the important first step in Endpoint Security since it allows administrators to get an assessment of the requesting device before granting logon.

Protected Resources

Ultimately, as the ever expanding virtual network grows, it is the internal corporate resources that require the most protection. Most organizations don't necessarily want all users' devices to get access to all resources all the time. Working in conjunction with the prelogon sequence, FirePass can gather device information (like IP address or time of day) and determine if a resource favorite should be offered. A protected configuration measures risk factors using information collected by the prelogon sequence; thus, they work in conjunction. 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, or 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 for each risk factor.

Figure 3: *Protection Criteria*

For instance, Fake Company Inc. has some contractors who need network access to Fake's corporate LAN. While this is not an issue during work hours, FCI does not want them looking around after dark. With the proper configuration, a contractor can log on at 10pm and FirePass can check the time; it already knows the 'contractor' network access favorite is only available during FCI's regular business hours, which happens to be 9am-5pm. The network access link he normally sees during regular business hours has vanished. If the user's endpoint protection does not satisfy the defined level, the system disallows access to resources.



Endpoint Security: *Protected Resources*

Fake may still allow access to certain web applications such as an extranet portal after hours, just not a full SSL VPN tunnel. The combinations can be endless but FirePass' Endpoint Security makes the daunting task seem elementary.

After determining, via prelogon inspection, that the device is safe, step two is to protect your resources.

Post logon

Post logon actions can protect against sensitive information being 'left' on the client. FirePass can impose a cache-cleaner to eliminate any user residue such as browser history, forms, cookies, auto-complete information and more. FirePass can close Google desktop search so nothing is indexed during the session. For systems unable to install a 'cleanup' control, configure FirePass to block all file downloads to avoid the possibility of the inadvertent left behind temporary file – yet still allow access to needed applications. Post logon actions are especially important when allowing non-trusted machines access without wanting them to take any data with them after the session.

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 typically a question of trust. Is there sufficient trust to allow a particular user and a particular device full access to enterprise resources? Endpoint Security gives the enterprise the ability to verify how much trust and determine whether the client can get all the resources, some of the resources, or none at all.

FirePass Integrated Endpoint Security provides:

- Automatic detection of security compliant systems, preventing infection
- Automatic integration with the largest number of virus scanning and personal firewall solutions in the industry (over 100 different AV 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 – reducing help desk calls
- A secure workspace, preventing eavesdropping and theft of sensitive data

- Secure login with a randomized key entry system, preventing keystroke logger snooping
- Full integration with the FirePass Visual Policy Editor. This enables the creation of custom template policies based on the endpoints accessing the network and the company's security profile

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast, and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability - all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.