

概述

随着 SSL VPN 技术日趋主流，企业允许外部的用户利用其内部基础设施，因此，端点安全性也就越来越受到关注。仅仅保护自己的资产免受恶意入侵者的攻击已经远远不够了。企业需要保护其资产，避免信任的员工从尚未安装补丁的家用电脑进行连接，还需要防止在开会时，这些员工在公用终端输入他们敏感认证凭证。

远程访问既变得更容易，同时也变得更加复杂。IPSec 通常仅供员工使用，它具有严格的设置和特定的端口，并且无需进行端点检查。SSL VPN 使任意用户都能够更轻松地连接到网络资源上，而由于同样的原因，也使其变得更加复杂。随着许多不同类型的用户通过各种各样的设备进行连接，同时访问大量不同的内部资源，要求对每个请求主体进行检查，以确保用户和设备都是值得信任的，这一点变得愈加重要。

挑战

SSL VPN 使远程访问向公众开放，而实现该访问所需的仅仅是一个浏览器，所以您不仅需要能够检测计算机类型（如，便携式电脑、PDA 或信息亭等），同时还必须能够检测其安全状况。由于市场上存在大量可访问互联网的设备，因此，在任意给定时刻，都可能会有 Windows 计算机、Linux 设备和 WAP 电话同时要求访问。在用户输入认证凭证前，对每个设备进行检测，以确保该设备是您允许访问的设备，这一点是非常必要的。如果检测失败，又如何解决这个问题以使用户可以具有某种等级的访问权限？如果请求主体是可允许访问的，您又如何决定哪些是他们有权访问的内容？并且，如果允许用户和设备进行访问，那么采用什么机制才能够保证他们没有带走或留下任何保密信息？关键的问题是确保仅有“安全”的系统才能访问您的高敏感基础设施。

实现该目标的第一步是列出使用环境。同安全策略配合使用，为不同类型的用户及他们可能使用的多种设备揭示使用环境和访问模式是非常重要的。下表是不同使用环境的一个很好的示例。

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

图 1：使用环境——资料来源：SSL VPN 中心

该图表可能会发生变化，但是这一练习可以使管理员开始制定端点计划。该图显示了用户类型、从何处进行连接、谁拥有并管理设备（如可能，还显示了设备类型）以及是否允许 ActiveX 或 Java 下载（通常用于运行端点检测器）。工作环境也可能发生改变，因为在某些时刻，通常通过公司电脑连接到 LAN 的“办公室工作人员”，可能需要在在一个开放的 Wi-Fi 系统上访问他们个人电脑里的资源。立即识别这种改变是非常重要的，因为用户虽然可能是有效用户，但他们的设备也许是不可信任的，这时您应该采用更精细的访问控制，仅允许他们访问通常访问的子集。

解决方案

允许受感染的设备访问网络，同允许无效用户访问专有内部信息一样糟糕。在这种情况下，可采用 F5 FirePass 强大的端点安全性。端点安全性可阻止已受感染的个人电脑、主机或用户设备与网络进行相连。对已受感染的个人电脑进行自动重新路由可减少呼叫帮助中心的次数，并防止按键记录器和恶意程序对敏感数据的窃取。

预登录检测

决定访问的第一步已不再是确认用户，而是首先检查用户正在使用的设备。预登录检测（见图 2）在实际登录页面出现之前运行，所以如果客户端不符合标准，则用户无法获得登录机会。这些检测和其它许多检测器一起，可以测定客户端设备是否运行

了防病毒软件或防火墙，以及这些软件是否为最新版本。

FirePass 可以将用户引导入纠正页面来获得更多指示，甚至还可以为用户打开防病毒软件或防火墙。检测器可以搜索特定的注册密码或文件（这些密码或文件是您公司电脑架构/映像的一部分），以决定它是否是公司的资产。预登录可以检索扩展的 Windows 和 IE 信息，以确保安装了某些特定的补丁。如果根据这些检测，FirePass 发现客户端不符合规定，但是用户是经过授权的用户，则它会为该会话创建一个安全的、受保护的工作区，并且使用户可以用安全虚拟键盘 (Secure Virtual Keyboard) 输入他们的敏感信息。该功能可利用 FirePass 易于使用的可视化策略编辑器 (Visual Policy Editor) 完成。

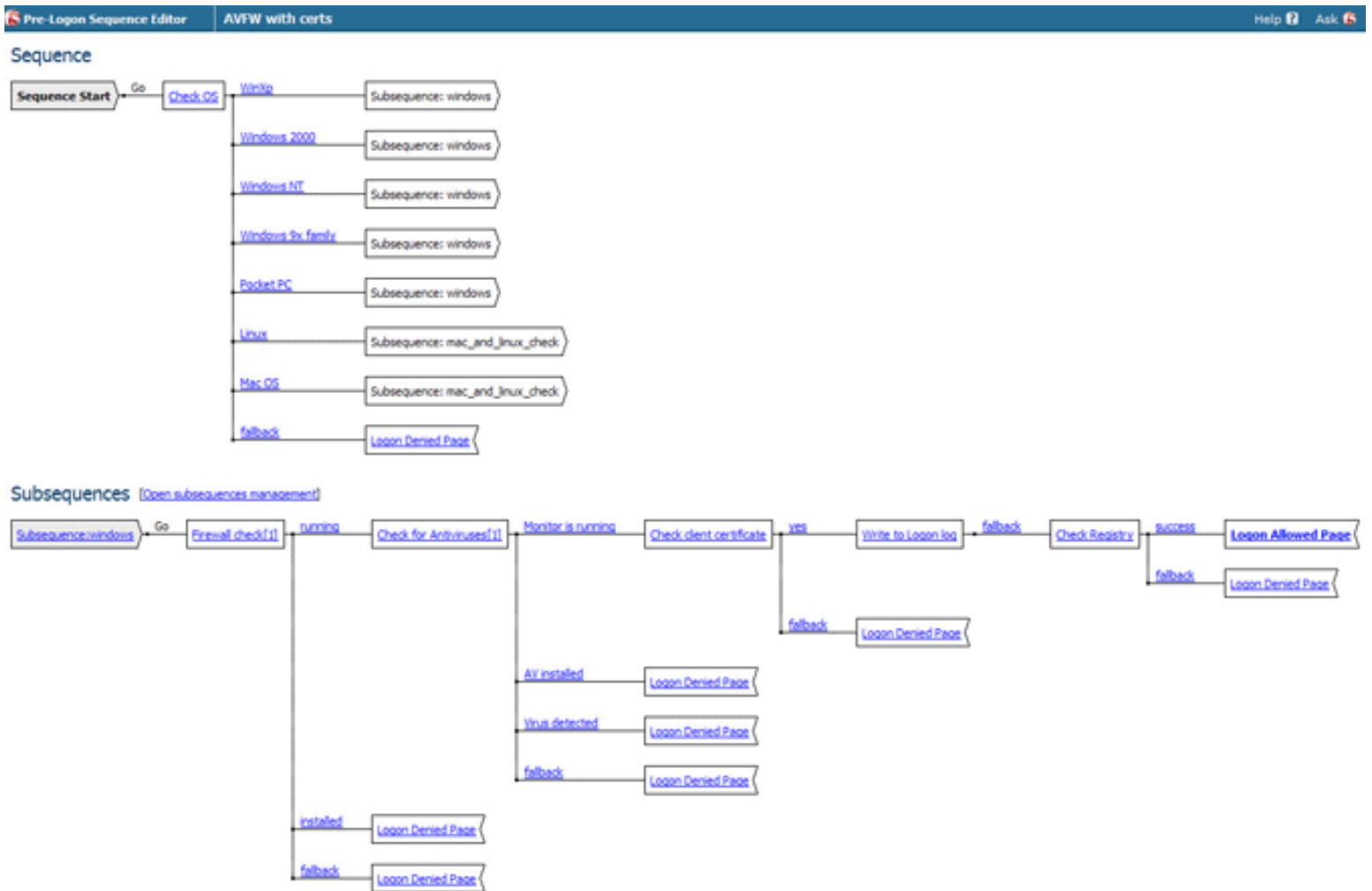


图 2: FirePass 预登录检测

可视化策略编辑器是一个简单的图形用户界面 (GUI)，它使复杂的执行简单化并灵活化。使用可视化策略编辑器，可以创建一个预登录安全策略，该策略可对每个要求登录 FirePass 控制网络的端点系统进行评估。FirePass 提供各种不同的预制模板，包括超过 25 个不同的防病毒/防火墙厂商、Google 桌面和客户端证书，用于对策略进行自动初始化。它还允许您以空白模板开始，从而进行完整的定制构建策略。管理员所需做的仅是“指向并点击”，即可建立规则，并根据结果采取行动。FirePass 集成的端点安全性为内置，但同样能够与第三方端点检测器共同使用，如，WholeSecurity 公司的 Confidence Online Server。

用户输入安全 FirePass 地址后，当收集关于最终用户系统的信息时，用户可以得到检测的可视化指示。预登录序列（见图 3）根据评估来决定激活哪个检测器。



图 3: FirePass 预登录序列

如果顺利，结果将会成功，用户可以进入登录页面。当然，另一个结果就是拒绝登录。告知用户发生失败的原因，以及解决问题的方法：“我们发现您安装了防病毒软件，但没有运行。请启用您的防病毒软件再进行访问。”在某些拒绝访问的例子中，FirePass 可以立即将客户端重新引导至纠正服务器。您可以将他们自动带入用来改正或更新用户软件环境的纠正网站，无需任何用户交互即可满足预登录检测所要求的策略，从而不必拒绝用户访问，并写出详细信息。

如果管理员对设备仍然不确定，或希望实现可控制的访问，那么就可以使用受保护的工作区。受保护工作区 (PWS) 允许您在客户访问 FirePass 上对最终用户打印、保存文件，或存储信息进行限制。它将用户限制在远程系统上临时的工作区内，该工作区包含临时的 Desktop (桌面) 和“My Documents (我的文档)”文件夹。在受保护模式下，用户不会无心地或意外地将文件写入到临时文件夹以外的位置。PWS 控制会在会话结束时删除临时工作区和所有的文件夹内容。当用户在不应该存储信息的设备上工作时，如不受 IT 控制的拇指驱动器 (thumb drive)，受保护工作区尤为有用。

预登录检测在端点安全性中，是非常重要的第一步，因为它使管理员能够在允许登录前对请求设备进行评估。

受保护的资源

最后，随着不断扩大虚拟网络的持续增长，企业的内部资源最需要受到保护。大部分企业并没有必要让所有的用户设备一直能够访问全部资源。和预登录序列配合使用，FirePass 可以收集设备信息（如，IP 地址或时间），从而决定是否提供资源。

一个受保护配置可以通过预登录序列收集的信息权衡风险因素，因此它们是配合使用的。FirePass 可以利用各种安全措施创建详细的受保护配置。它可以检测到一个登录是否来自可信任的网络，端点运行的是什么防病毒软件，或客户端正在使用的是哪种认证方式。大量不同的检测涵盖了保护标准（见图 3），如，键盘记录器 (logger)、病毒感染、信息泄露以及非法访问。然后，管理员可以为每种风险因素选择所需要的安全特性。

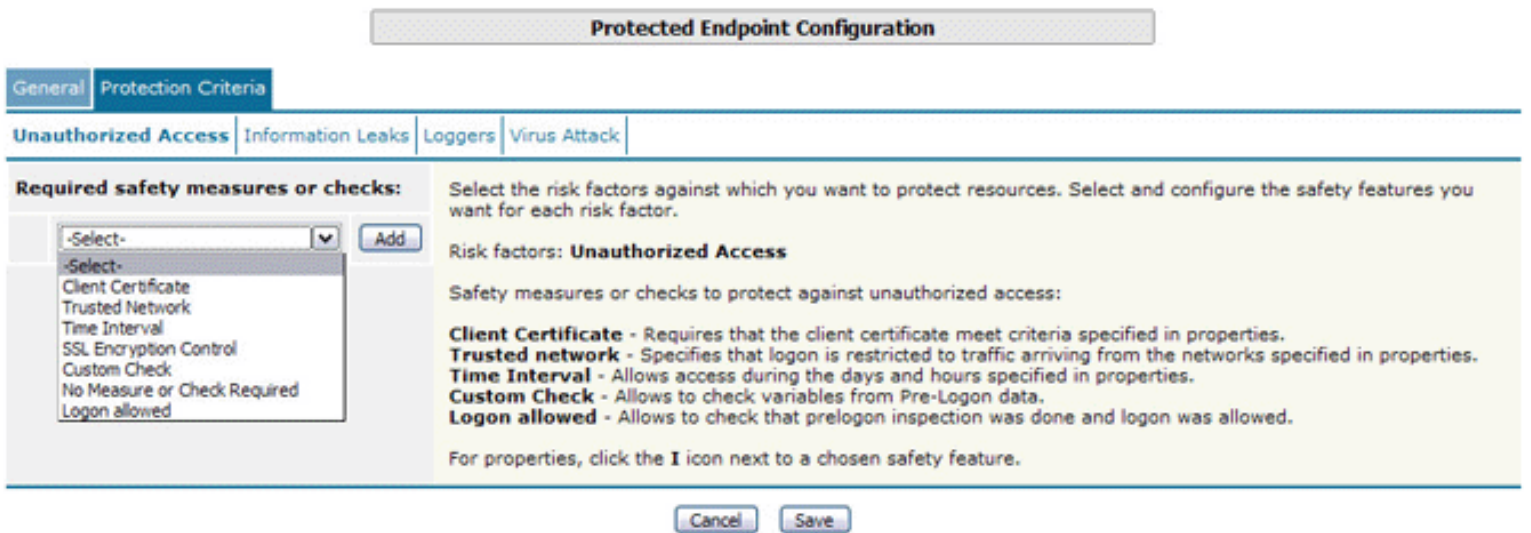


图 4：保护标准

例如，ABC 公司有一些承包商需要能够访问 ABC 的企业 LAN。这在工作时间并不是什么问题，但是 FCI 不希望在下班后这种访问还继续。通过恰当的配置，承包商可以在下午 10 点登录，FirePass 能够检测到该时间；它还知道只有在正常的工作时间内“承包商”才能够访问他们所需的资源，这一时段是从上午 9 点到下午 5 点。“承包商”在正常工作时间能够看到的网络访问链接现在已经消失了。如果用户的端点保护不能满足定义的等级，则系统将不允许用户访问资源。

Protect Resources

Resource	Required protection	
Firepass Webtop		Select
Web Application Tunnels		Select
Network Access		Select
Connection in Endy_test		Select
Connection in F5Resources		
Connection in psilva		
Connection in sdrack	time	
Connection in ssa_resource		
AppTunnels		Select
Legacy Hosts		Select
Terminal Servers		Select
Web Applications		Select
Windows Files		Select

Resource group	Required protection	
Default_resource	time	Select
Endy_test		Select
F5Resources		Select
psilva		Select
sdrack		Select
ssa_resource		Select

图 5：端点安全性：受保护的资源

ABC 公司可能允许“承包商”在工作时间后访问某些 web 应用（如，外联网门户），但不是完整的 SSL VPN 隧道。这种组合可能是无止境的，但 FirePass 端点安全性使这望而生畏的工作变得非常简单。

当通过预登录检测，并确定设备是安全的，则第二步就是保护您的资源。

登录完毕后

登录后操作可以保护敏感的信息不被“遗留”在客户端上。FirePass 可以利用高速缓存清除器清除所有用户遗留下的信息，如浏览器的历史记录、窗口、cookies、自动完成信息以及其它更多内容。FirePass 能够关闭 Google 桌面搜索，因此在会话过程中任何信息都不会被编入索引。对于不能安装“清除”控制的系统，可以配置 FirePass，以拦截所有的文件下载，从而避免无意中遗

留临时文件的可能，同时仍允许访问所需的应用。对于那些允许不可信任设备访问，但不希望它们在会话后保留任何数据的情形，登录后操作显得尤为重要。

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.](#)

图 6：登录后操作

总之：第一步，检测请求设备；第二步，依据检测中获取的数据对资源进行保护；第三步，确保没有留下任何会话遗留信息。

结论

典型地，安全是信任的问题。是否存在足够的信任，能够允许某个特定的用户和特定的设备对企业资源进行完全访问？端点安全性使企业能够核实信任的程度，从而决定客户端可以访问全部资源、部分资源还是根本不允许访问。

FirePass 集成的端点安全性提供了：

- ☆ 安全兼容系统自动检测，防止受到感染
- ☆ 与业内数量最多的病毒扫描及个人防火墙解决方案（超过 100 种不同的防病毒和个人防火墙版本）自动集成。
- ☆ 自动拦截受感染的文件上传或电子邮件附件
- ☆ 自动重新路由并隔离受感染或非标准的系统，将其放入自我补救网络中 (self remediation network)——以减少呼叫帮助中心的次数。

☆ 安全工作区可阻止窃听及窃取敏感数据

☆ 使用随机键输入系统进行安全登录可防止按键记录器的窃听

☆ 由于能够与 FirePass 可视化策略编辑器完全集成因此，可创建基于端点访问您的网络及您公司的安全配置文件的定制模板策略