HCIE-Security 备考指南

终端安全（SVN）

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目　录

HCIE-Security 终端安全（SVN）需要掌握的知识点

■ 掌握 SSL VPN 终端安全配置

终端安全简介

终端安全包括用户接入虚拟网关时的主机检查和用户退出时的缓存清理。

终端安全通过定义主机检查策略和缓存清理策略来实现：

- 主机检查策略主要用于检查用户接入虚拟网关的主机是否符合安全要求，包括操作系统、端口、进程、杀毒软件、防火墙软件、注册表以及是否存在指定文件。另外还提供以下功能：
  - 防二次跳转

    检查客户端是否开启远程共享程序，以防止客户端被其他 PC 远程控制。
  - 防截屏

    检查客户端是否开启截屏程序，避免泄露机密信息。
- 缓存清理策略主要用于清理用户访问内网过程中在终端上留下的访问痕迹，包括：
  - 清除生成的临时文件、自动保存的密码、Cookie 记录、浏览器历史记录、回收站以及最近打开文档列表。
  - 禁用 IE 浏览器的表单自动完成功能和地址栏自动完成功能。
  - 自定义清理特定的文件或文件夹。

配置主机检查

您需要启用主机检查功能，并配置主机检查策略。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 终端安全 > 主机检查”。
3. 启用主机检查功能。
   a. 在“全局配置”区域框中，选中“主机检查功能”对应的“启用”。

b. **可选**：根据需要选中“防二次跳转”和“防截屏”对应的“启用”。

说明：

启用防二次跳转和防截屏功能后，除了默认可以防御的远程共享程序和截屏程序，您还可以通过配置主机规则定义其他可以防御的程序。

- 启用“防二次跳转”后，可检查客户端是否开启远程共享程序，以防止客户端被其他 PC 远程控制。

  开启防二次跳转功能后，默认可以防御以下远程共享程序：

  - mstsc（Microsoft Terminal Services Client）
  - pcanywhere
  - VNC

- 启用“防截屏”后，检查客户端是否开启截屏程序，避免泄露机密信息。

  开启防截屏功能后，默认可以防御以下截屏程序：

  - PrintScreen
  - HyperSnap
  - SnagIt
  - EasyCapture
  - SnippingTool
  - 红蜻蜓抓图精灵
  - 晨风

c. 单击“应用”。

d. 在操作成功的提示框中。单击“确定”。

4. 配置主机检查策略。

a. 在“主机检查策略列表”区域框中，单击“新建”。

b. 在“策略名”和“描述”中分别输入策略的名称和描述。

策略名中不能包含以下字符：（、）、&、|、^。

c. 配置策略的通过条件：

- 选中“满足以下所有规则”，表示只有当策略下的规则全部检查通过时，策略检查通过。
- 选中“满足以下任一规则”，表示只要策略下有任意一条规则检查通过，策略检查通过。
- 选中“自定义”，通过输入操作符来配置策略通过条件。

  支持&、|、(、)四个操作符。例如：rule1&(rule2|rule3)表示只有满足规则 rule1，同时满足 rule2 或 rule3 才能通过策略检查。

d. 配置主机检查规则。

1. 在“规则列表”中，单击“新建”。
2. 在“规则名”中输入规则的名称。

   说明：

   规则名中不能包含以下字符：(、)、&、|、^。

3. 在“规则类型”中选择需要检查的项并配置具体的规则，然后单击“确定”。

规则类型	说明
杀毒软件	1. 选择“规则类型”为杀毒软件。 2. 指定杀毒软件。 • 选中“任何支持的杀毒软件”，表示只要被检查的用户终端上安装并运行了任一支持的杀毒软件版本，即可通过规则检查。 • 选中“指定杀毒软件”，并将需要支持的杀毒软件的版本加入“指定杀毒软件列表”。表示只有被检查的用户终端上安装并运行了任一“指定杀毒软件列表”中的杀毒软件版本，才可通过规则检查。
防火墙软件	3. 选择“规则类型”为防火墙软件。 4. 指定防火墙软件。 • 选中“任何支持的防火墙软件”，表示只要被检查的用户终端上安装并运行了任一支持的防火墙版本，即可通过规则检查。 • 选中“指定防火墙软件”，并将需要支持的防火墙版本加入“指定防火墙软件列表”。表示只有被检查的用户终端上安装并运行了任一“指定防火墙软件列表”中的防火墙版本，才可通过规则检查。 **说明：** 当将“Windows 防火墙”列入“指定防火墙软件列表”时，如果用户终端上安装的操作系统为 Windows 7，必须启用当前所使用的网络类型的 Windows 防火墙，才能通过主机检查策略。
操作系统	5. 选择“规则类型”为操作系统。 6. 选中要支持的操作系统前的复选框，并配置最小 SP（Service Pack）版本。最小 SP 版本指 Windows 支持的最小补丁版本。

规则类型	说明
	例如：选中 Windows 2003 后，不选中“必须至少打过”，表示 Windows 操作系统为 Windows 2003 以及 Windows 2003（SP1、SP2）的操作系统都能通过规则检查。如果选中“必须至少打过”，并选择“SP2”，那么只有操作系统为 Windows 2003 SP2 才能通过规则检查，Windows 2003 SP1 及以下版本不能通过规则检查。
端口	7. 选择“规则类型”为端口。 端口指用户终端开放的端口。 8. 在“端口”中输入端口号。 9. 配置规则行为： • 选择“需要开放”，表明只有开放这些端口的用户终端能通过规则检查。 • 选择“不允许开放”，表明未开放这些端口的用户终端才能通过规则检查。
进程	10.选择“规则类型”为进程。 进程指在用户终端上运行的进程。 11.在“进程名”中输入进程的名称。 12. 配置规则行为： • 选择“需要开启”，表明只有运行这些进程的用户终端能通过规则检查。 • 选择“不允许开启”，表明未运行这些进程的用户终端才能通过规则检查。 选中“如果该进程存在，结束该进程”，强制关闭进程。关闭进程后，允许用户终端通过规则检查。 13.**可选：**在“MD5 校验值”中单击“选择文件并解析 MD5 值”选择进程的可执行文件，解析该进程的 MD5 值。 由于进程的名称可能会被恶意更改，导致采用进程名的规则无效。使用能唯一标识进程的 MD5 值进行校验能更好地确保进程规则的有效性。解析 MD5 值后，进行主机检查时，设备根据进程名和进程的 MD5 值检查进程是否存在，确保进程检查的有效性。
文件	14.选择“规则类型”为文件。 文件指在用户终端上的文件。 15.在“文件位置”中输入文件的详细路径。 **说明：** “文件位置”必须与用户 PC 中的文件路径完全一致，否则规则无效。 “文件位置”支持输入目录宏。各目录宏对应的文件详细路径如表 1 所示。例如，如果要检查系统 C 盘根目录下的文件 1.txt，可以输入 C:\1.txt，或使用目录宏，输入%HOMEDRIVE%\1.txt。 如果要检查系统 Temp 文件夹下所有后缀名为.tmp 的文件，可以输入 C:\Documents and Settings\Administrator\Local Settings\Temp*.tmp，或使用目录宏，输入%TEMP%*.tmp。 16.配置规则行为： • 选择“需要存在”，表明存在这些文件的用户终端能通过规则检查。 • 选择“不需要存在”，表明不存在这些文件的用户终端才能通过规则检查。

规则类型	说明
	选中“如果该文件存在，清除该文件”，强制用户删除存储在用户终端上的文件。清除文件后，允许用户终端通过规则检查。 17.**可选：**在“MD5 校验值”中单击“选择文件并解析 MD5 值”选择文件，解析该文件的 MD5 值。 由于文件的名称可能会被恶意更改，导致采用文件名的规则无效。使用能唯一标识文件的 MD5 值进行校验能更好地确保文件规则的有效性。解析 MD5 值后，在进行主机检查时，设备根据文件名和文件的 MD5 值检查文件是否存在，确保文件检查的有效性。
注册表	18.选择“规则类型”为注册表。 19. 配置注册表的详细信息。 选中“如果检测到与上述设定的值不符合的项，强制将注册表项自动修改为上述设定的值”后，如果用户终端的注册表信息与在设备上配置的注册表信息不一致，将强制修改用户终端的注册表信息为设备上配置的注册表信息，并允许用户终端通过规则检查。 **说明：** 当注册表的表项名为空时即为默认的注册表表项。 配置注册表规则后，当用户终端的注册表和设置的注册表一致时，用户终端才能通过规则检查。
防二次跳转	指定终端上禁止运行的远程共享程序。远程共享程序可以通过以下方式来指定： • “应用程序窗口名”：指定远程共享程序的窗口名称。 • “端口”：指定远程共享程序的使用的端口号。 • “MD5 校验值”：应用程序或文件的名字可以修改，导致采用名字识别的方式会失效。此时，建议采用 MD5 方式。MD5 值能唯一标识某个程序或文件。
防截屏	指定终端上禁止运行的截屏程序。截屏程序可以通过以下方式来指定： • “应用程序窗口名”：指定截屏程序的窗口名称。 • “MD5 校验值”：应用程序或文件的名字可以修改，导致采用名字识别的方式会失效。此时，建议采用 MD5 方式。MD5 值能唯一标识某个程序或文件。
防截屏白名单	指定终端上允许注册截屏键（PrintScreen、Alt+PrintScreen、Ctrl+PrintScreen）的程序，即该程序可以注册截屏键。白名单中程序可以通过以下方式来指定： • “进程名”：指定程序的进程名称。 • “MD5 校验值”：可以手动在文本框中输入 MD5 值，或通过解析进程可执行文件获取 MD5 值。MD5 值能唯一标识某个程序或文件。 **说明：** 某些非截屏程序也会注册截屏键。防截屏功能开启后，安装了这些软件的终端将不能接入网络。此时可以将这些软件添加到防截屏白名单中。

表 1 目录宏介绍

目录宏	详细路径
%APPDATA%	C:\Documents and Settings\<user name>\Application Data

规则类型	说明
%windir%	C:\WINDOWS
%ProgramFiles%	C:\Program Files
%CommonProgramFiles%	C:\Program Files\Common Files
%USERPROFILE%	C:\Documents and Settings\<user name>
%HOMEDRIVE%	C:
%Temp%	C:\Documents and Settings\<user name>\Local Settings\Temp
%ProgramW6432%（只有 64 位操作系统支持该宏）	C:\Program Files
%CommonProgramW6432%（只有 64 位操作系统支持该宏）	C:\Program Files\Common Files
说明： 假设操作系统安装在 C 盘。 <user name>为当前操作系统用户的名称。	

e. 单击“确定”。

5. 关联角色和主机检查策略，请参见配置角色。

配置缓存清理

您需要启用缓存清理功能，并配置需要清理的缓存内容。

配置缓存清理

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 终端安全 > 缓存清理”。
3. 在“缓存清理配置”区域框中，选中“启用缓存清理”。
4. 根据需要清理的内容选择清理选项（假设操作系统安装在 C 盘；<user name>为当前操作系统用户的名称）。

说明：

如果用户终端是多人共用的 PC 或用户终端使用环境为网吧等公共场所，建议选中所有选项。

参数	说明
退出时清除 Internet 临时文件	选中表示删除 Internet 临时文件夹里面的所有内容。 不同的网络浏览器，Internet 临时文件储存的位置也不同： • IE（Internet Explorer） C:\Documents and Settings\<user name>\Local Settings\Temporary Internet Files. • FireFox C:\Documents and Settings\<user name>\Local Settings\Application Data\Mozilla\Firefox\Profiles\iyic56oc.default\Cache
退出时清除自动保存的密码	选中表示删除网络浏览器在访问虚拟网关过程中自动保存的密码。 不同的网络浏览器，密码储存的位置也不同： • IE 自动保存的密码位于注册表。 • FireFox C:\Documents and Settings\<user name>\Application Data\Mozilla\Firefox\Profiles*.default\signons3.txt
退出时清除 Cookie 记录	选中表示删除网络浏览器在访问虚拟网关过程中产生的 Cookie 记录。 不同的网络浏览器，Cookie 记录储存的位置也不同： • IE C:\Documents and Settings\<user name>\Cookies • FireFox C:\Documents and Settings\<user name>\Application Data\Mozilla\Firefox\Profiles*.default\cookies.sqlite **说明：** Cookie 是 Web 服务器存储和检索来自客户端（浏览器）信息的一种机制。Cookie 由服务器生成，然后发送到客户端。如果被接受，下一次客户端再连接到这项服务时，客户端的计算机就会自动将此信息送给服务器。但 Cookie 中保存了客户端的信息，存在安全隐患。
退出时清除浏览器的历史记录	选中表示删除浏览器的所有历史记录。 历史记录储存的位置：C:\Documents and Settings\<user name>\Local Settings\History
退出时清除回收站和最近打开文档列表	选中表示删除回收站和最近打开的文档列表中的所有内容。 最近打开文件列表路径为 C:\Documents and Settings\<user name>\Recent。注册表中的最近打开文件列表也会被删除。
禁用基于 IE 的网络浏览器的表单自动完成功能	表单自动完成功能记录用户在网页上建立的全部条目，这些条目中保存着私人信息，其他人可能查看到这些私人信息。 选中表示禁止基于 IE 的网络浏览器保存用户建立的条目。
禁用基于 IE 的网络浏览器的地址栏自动完成功能	地址栏自动完成功能记录用户输入的 Internet 地址，在输入 Internet 地址时网络浏览器会自动提供建议的地址，方便用户访问。但地址栏自动完成功能会泄漏用户访问的信息。 选中表示禁止基于 IE 的网络浏览器保存 Internet 地址。

5. 单击“确定”。

6. 在操作成功的提示框中。单击“确定”。

清理指定文件或文件夹

某些文件或文件夹包含敏感信息，通过配置此功能，用户在退出虚拟网关时，自动删除指定文件或文件夹。

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 终端安全 > 缓存清理”。
3. 在“清除指定的文件或文件夹列表”区域框中，单击“新建”。
4. 在“文件或文件夹路径”中输入需要删除的文件路径或文件。

   路径支持目录宏，包括%USERPROFILE%和%Temp%。

   例如，如果要删除系统 Temp 文件夹下的文件 1.txt，可以输入 C:\Documents and Settings\Administrator\Local Settings\Temp\1.txt，或使用目录宏，输入%Temp%\1.txt。

目录宏	说明
%USERPROFILE%	系统用户文件夹。假设 C 盘为系统盘，路径为 C:\Documents and Settings\<user name> **注意：** 请谨慎使用该宏，使用不当，可能造成系统或某些程序无法正常运行。
%Temp%	系统临时文件夹。假设 C 盘为系统盘，路径为 C:\Documents and Settings\<user name>\Local Settings\Temp

   文件名支持通配符“?”和“*”。

   - 星号（*）：可以使用星号代替零个或多个字符。对于要删除的文件，如果您知道文件包含字母“temp”，但不记得文件名的其余部分，则可以键入以下字符串：*temp*，这样会删除文件名包含“temp”的所有文件类型的所有文件，如 Intenettemp.txt、extemper.doc 等。
   - 问号（?）：可以用问号代替名称中的零个或单个字符。例如，当键入“temp?.doc”时，删除的文件可能为 temp.doc 或 temp1.doc，但不会是 temper.doc。

   例如，如果要删除系统 Temp 文件夹下所有后缀名为.tmp 的文件，可以输入 C:\Documents and Settings\Administrator\Local Settings\Temp*.tmp，或使用目录宏，输入%TEMP%*.tmp。

   注意：

   不要直接输入%Temp%，这样可能会删除 Temp 文件夹下的所有文件。

5. 选择是否删除子文件夹。

   - 选中“删除子文件夹”，删除路径下的所有文件及文件夹。

- 取消选中“删除子文件夹”，只删除路径下的文件，不删除文件夹。

6. 单击“确定”。

HCIE-Security 模拟面试问题及面试建议

1. SVN 终端安全有哪些？