防火墙迁移工具常见问题

防火墙迁移工具常见问题

防火墙迁移工具常见问题解答

问： 版本 3.0.1 的 Cisco Secure Firewall 迁移工具支持哪些新功能？

答： Cisco Secure Firewall 迁移工具 3.0.1 现在仅支持将 Cisco Secure Firewall 3100 系列作为从 Check Point 迁移的目标设备。

问： 版本 3.0 的 Cisco Secure Firewall 迁移工具支持哪些新功能？

答： 迁移到云交付的防火墙管理中心

问： 版本 2.5.2 的 Cisco Secure Firewall 迁移工具支持哪些新功能？

答： Check Point 的 ACL 优化。

问： 从 Check Point 转换到 FTD 有哪些硬件限制？

答： 如果配置文件与 Check Point Web 可视化工具以及 FMT-CP-Config-Extractor_v3.0.1-7373 工具兼容，则您应该能够迁移源 Check Point。

问： 是否可以使用从 Check Point r76SP 导出的配置并将其迁移到 4100 和 6100 Firepower 平台？

答： 是。所有平台均支持 r75 至 r77.30。

只要提供了 Check Point Web 可视化工具，就能支持该平台。

问： 如何处理 Check Point 规则中的否定对象？

答： 如果对象属于排除类型对象/组，则 ACL 转换遵循 **permit** 和 **block** 组合。尽管不支持排除类型的网络对象/组，但 ACL 支持该转换。例如，在 Check Point ACE 规则引用了排除类型的对象组时。

- 如果 Check Point 规则操作为 **permit**：
  - ACE 必须对 **<exception></exception>** XML 标记下引用的对象组的 **Deny** 执行一个操作，在规则附加一个例外对象组规则注释。

- ACE 必须对 <*base*><*/base*> XML 标记下引用的对象组的 **Allow** 执行一个操作，在规则附加一个例外对象组规则注释。

- 如果 Check Point 规则操作为 **Deny/Reset**：
  - ACE 必须对 **<exception></exception>** XML 标记下引用的对象组的 **permit** 执行一个操作，为规则附加一个“例外对象组规则”注释。
  - ACE 必须对 **<base></base>** XML 标记下引用的对象组的 **Block(Deny)/Block** with **Reset(Reject)** 执行一个操作，在规则附加一个例外对象组规则注释。

问: 防火墙迁移工具是否支持带否定单元的 ACE？如果不支持，防火墙迁移工具会如何处理这些规则？

答: 防火墙迁移工具不支持具有否定单元的 ACE，它们通过将 ACE 视为普通 ACE 来进行转换。这些问题将在后续版本中加以解决。

问: 您看到“未能绑定到数据库。访问被拒绝”错误。您该怎么做？

答: 请执行以下操作：

- 打开管理服务器的 Check Point Gaia 控制台。
- 导航至 Gaia 控制台上的用户和角色设置。
- 在具有管理员角色的 Check Point 管理服务器 Gaia 控制台上使用主目录 `/home` 和 Shell `/etc/cli.sh` 参数的创建一个新的用户名凭证。

问: 在通过防火墙迁移工具解析 Check Point 配置时，您会看到解析计数为 0。您该怎么做？

答: 执行以下任一步骤：

使用 FMT-CP-Config-Extractor_v3.0.1-7373 工具解压缩 *network.txt* 文件，并要避免使用手动编码的 *network.txt* 文件。

或

有可能出于任何原因而在 Check Point 安全网关上启用日志记录，从那里输出的 *network.txt* 文件会被导出。由于启用了日志记录，在 *network.txt* 文件中添加的无关信息会导致此类问题。如果是这样，请执行以下操作：

- 检查 *network.txt* 文件。
- 通过删除附加的额外日志行来修复文件。
- 将新的压缩文件上传到防火墙迁移工具。

问: 是否可以使用 VSX 从 Check Point 迁移配置？

答: 您可以导出与虚拟系统相关的特定策略包，一次只能从一个虚拟系统导出。例如，当您使用 Web 可视化工具 (r75 – r77.30) 导出配置时，它就会导出所有虚拟系统的策略元素。因此，请仅保留要迁移的虚拟系统的 NAT 和策略文件，以及 *index.xml*、*community.xml*、*network_objects.xml* 和 *network.txt*（从要迁移的策略的安全网关），以便让配置保持完整。

对于 r80，当您通过 Live Connect 连接到 Check Point 安全管理器时，选择特定虚拟系统的策略包，这就是在您选择 Check Point 策略包并推导出配置时要在第 5 步中迁移的策略包。

当您还连接到 Check Point 安全网关时，请提供与 Check Point 策略包对应的正确 Check Point 虚拟系统 Check Point 防火墙包的正确详细信息。

如果仍然遇到问题，请联系思科 TAC 为这些故障创建 TAC 案例。

问： 您能否手动提取 Check Point (r80) 配置？

答： 不能。无法手动提取 Check Point (r80) 配置。使用防火墙迁移工具上的 Live Connect 可导出完整的 r80 配置。当您使用手动变通方法提取配置或使用未在防火墙迁移工具中配置的 Check Point (r80) 配置时，该配置是不完整的，并且也会作为不受支持的配置进行迁移、被部分迁移，甚至导致迁移失败。

有关详细信息，请参阅导出 Check Point r80 配置文件。

问： 为不同的 Check Point (r80) 部署类型预先配置凭证的方式有哪些？

答： 迁移前，您可以通过以下任何一种方式在 Check Point (r80) 设备上配置凭证：

- 从分布式 Check Point 部署导出
- 从独立 Check Point 部署导出
- 在多域部署中导出 Check Point (r80)

问： 我在 Check Point r80 上为 Check Point 安全管理器使用了自定义 API 端口。我必须怎样做才能完全提取配置？

答： 如果您在 Check Point 智能管理器上使用客户 API 端口来使用 Check Point API，请执行以下步骤：

- 在 Live Connect 的 **Check Point 安全管理器**页面上，选中 **Check Point 多域部署**复选框。
- 如果使用多域部署，请添加 Check Point CMA 的 IP 地址和 API 端口详细信息。
- 如果是常规部署，请保留 Check Point 安全管理器的 IP 地址，并输入自定义 API 端口的详细信息。

问： 我有一个 r80.40 版本的 Check Point 网关，并且通过 Live Connect 能够正常提取。但在解析时，我收到了错误消息：“Blocked VSX Feature is UNSUPPORTED in FTD”。我必须怎样做？

答： 之所以出现该错误是因为从 Check Point r80.40 开始弃用了 **fw vsx stat** 命令。在解析 *network.txt* 文件时，防火墙迁移工具在执行 **fw vsx stat** 命令后将无法对值进行解析。

解决方法是执行以下步骤：

1. 解压缩 *config.zip* 文件。
2. 打开 *networking.txt* 文件。

   以下是样本输出的示例：

```
firewall> fw vsx stat
Deprecated command, Please see sk144112 for alternative
Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
```

按照如下步骤手动进行更换：

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. 选择所有文件并以 .zip 扩展名将它们压缩。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。