为具有HairPin流量的FTD上的VPN用户配置内部资源访问

目录

问题

目标是在Cisco安全防火墙FTD上使用RADIUS（针对Windows加入域的服务器）成功进行VPN身份验证后，使VPN用户能够完全访问内部网络资源。

VPN设置已可操作；用户可以下载并安装VPN客户端并成功进行身份验证。问题的重点是配置必要的访问控制和NAT规则以允许通过VPN访问所需的内部资源。

环境

- 产品：Cisco Secure Firewall Firepower(FTD)，版本7.6.0（例如CSF1220CX设备）
- 管理：Firepower管理中心(FMC)、云交付FMC(cdFMC)或Firepower设备管理器(FDM)
- VPN：配置为针对Windows加入域的服务器(NPS)进行RADIUS身份验证
- VPN地址池：192.168.250.1 - 192.168.250.200
- 目标内部子网示例：192.168.95.0/24
- 软件版本：9.22.1（如工作流程中所述）
- 相关接口：VPN入口的“外部”接口
- 需要通过VPN连接进行RDP和Active Directory访问

分辨率

这些步骤详细说明了允许VPN用户访问Cisco FTD上的内部资源（如RDP和Active Directory）所需的配置。这包括创建访问策略规则、为VPN流量配置NAT豁免和发夹NAT，以及使用故障排除命令验证配置。

第1步：添加访问列表条目以允许VPN地址池访问内部资源。

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

第2步：添加访问列表规则，以允许内部资源将返回流量发送到VPN池：

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

以后可根据需要收紧这些规则，以限制特定源和目标。

第3步：为VPN流量配置NAT免除或发夹NAT

有两种常用方法：

- 选项A:VPN池到内部子网的NAT免除

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- 选项B：同一接口上VPN池的发夹NAT(no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- 选项C：外部接口上VPN池的动态发夹NAT

```
nat (outside,outside) dynamic VPN_Pool interface
```

正确的方法取决于内部资源是位于同一物理接口（需要发夹NAT）还是不同接口（NAT免除）。

第4步：使用packet-tracer命令模拟从VPN池到内部资源的流量，并验证目标规则、NAT和路由是否允许流量。

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

注意：WebVPN阶段的Packet Tracer输出可能对外部接口上的VPN流量显示“DROP”。这是外部接口上的纯文本流量的预期行为，仍可用于验证NAT。

其他说明：

- 威胁防御UI中的数据包捕获可能只显示传入请求。如果未观察到丢包，但流量未到达内部资源，请检查NAT和访问列表规则。
- 当SSH不可用时，可通过cdFMC中的威胁防御UI功能执行所有故障排除，但命令使用受到限制。
- 可能需要对相邻设备进行一些修改，以实现端到端连接。

原因

根本原因是VPN到内部和内部到VPN池流量的访问策略和NAT配置不足。默认配置不允许从VPN池到内部资源以及回传的完全双向通信，也不处理同一接口上流量传入和传出的发夹NAT要求。

相关内容

- 在FTD上配置NAT免除
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。