在安全防火墙ASA上配置远程访问VPN服务的威胁检测

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 尝试连接到仅内部（无效）VPN服务的威胁检测
- 远程访问VPN客户端发起攻击的威胁检测
- 远程访问VPN身份验证失败的威胁检测

验证

相关信息

简介

本文档介绍在思科安全防火墙ASA上为远程访问VPN配置威胁检测功能的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure Firewall 自适应安全设备 (ASA)
- ASA上的远程访问VPN(RAVPN)

以下思科安全防火墙ASA版本支持以下威胁检测功能：

- 9.16版本系列>支持9.16(4)67及此特定系列中的更新版本。
- 9.17版本系列>支持9.17(1)45及此特定系列中的更新版本。
- 9.18版本系列>支持9.18(4)40及此特定系列中的更新版本。
- 9.19版本系列>支持9.19(1)。37及此特定系列中的更新版本。

- 9.20版本系列>支持9.20(3)及此特定系列中的更新版本。
- 9.22 version train > supported from 9.22(1.1)及任何更新版本。

注:9.22(1)未发布。第一个版本为9.22(1.1)。

使用的组件

本文档中描述的信息基于以下硬件和软件版本：

- 思科安全防火墙ASA版本9.20(3)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

针对远程访问VPN服务的威胁检测功能通过自动阻止超过配置阈值的主机（IP地址），帮助阻止来自IPv4地址的拒绝服务(DoS)攻击，从而阻止进一步尝试，直到您手动删除IP地址回避为止。有单独的服务可用于以下类型的攻击：

- 对远程访问VPN服务重复失败的身份验证尝试（暴力用户名/密码扫描攻击）。
- 客户端发起攻击，攻击者从单个主机开始尝试连接远程访问VPN头端，但尝试连接未完成。
- 连接尝试无效的远程访问VPN服务。也就是说，当攻击者尝试连接到仅用于设备内部运行的特定内置隧道组时。合法终端永远无法尝试连接到这些隧道组。

这些攻击，即使尝试访问时失败，也会消耗计算资源，并阻止有效用户连接到远程访问VPN服务。

当您启用这些服务时，安全防火墙会自动避开超过配置阈值的主机（IP地址），以防止进一步尝试，直到您手动删除IP地址的回避。

注意：默认情况下会禁用远程访问VPN的所有威胁检测服务。

配置

在全局配置模式下登录到安全防火墙命令行界面(CLI)，并为远程访问VPN启用一个或多个可用的威胁检测服务：

尝试连接到仅内部（无效）VPN服务的威胁检测

要启用此服务，请运行threat-detection service invalid-vpn-access命令。

远程访问VPN客户端发起攻击的威胁检测

要启用此服务，请运行threat-detection service remote-access-client-initiations hold-down <minutes> threshold <count>命令，其中：

- hold-down <minutes>定义最后一次启动尝试后的时段，在该时段内计算连续的连接尝试。如果在此时间段内连续连接尝试次数达到配置的阈值，则避开攻击者的IPv4地址。您可以将此时间设置为1到1440分钟之间。
- threshold <count>是在抑制期间内触发回避所需的连接尝试次数。可以将阈值设置为5和100。

例如，如果抑制期为10分钟，阈值为20，则如果在任何10分钟跨度内连续尝试20次连接，将自动避免使用IPv4地址。

注意：设置抑制和阈值时，请考虑NAT使用情况。如果使用PAT（允许来自同一IP地址的许多请求），请考虑更高的值。这可确保有效用户有足够的时间进行连接。例如，在酒店中，许多用户可以在短时间内尝试连接。

远程访问VPN身份验证失败的威胁检测

要启用此服务，请运行threat-detection service remote-access-authentication hold-down<minutes> threshold <count>命令，其中：

- hold-down <minutes>定义最后一次失败尝试后统计连续失败的时间段。如果在此时间段内连续身份验证失败次数达到配置的阈值，攻击者的IPv4地址将被回避。您可以将此时间设置为1到1440分钟之间。

- threshold <count>是在抑制期间内触发回避所需的身份验证失败尝试次数。可以将阈值设置为1和100。

例如，如果抑制期为10分钟，阈值为20，则如果任何10分钟跨度内连续发生20次身份验证失败，将自动避免使用IPv4地址。

注意：设置抑制和阈值时，请考虑NAT使用情况。如果使用PAT（允许来自同一IP地址的许多请求），请考虑更高的值。这可确保有效用户有足够的时间进行连接。例如，在酒店中，许多用户可以在短时间内尝试连接。

注意：尚不支持通过SAML进行身份验证失败。

下一个示例配置为远程访问VPN启用三个可用的威胁检测服务，抑制时间为10分钟，客户端发起和失败的身份验证尝试的阈值为20。

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

验证

要显示威胁检测RAVPN服务的统计信息，请运行show threat-detection service [service] [entries|details]命令。服务的位置：remote-access-authentication、remote-access-client-initiations或invalid-vpn-access。

您可以通过添加以下参数进一步限制视图：

- entries — 仅显示威胁检测服务正在跟踪的条目。例如，身份验证尝试失败的IP地址。
- 详细信息 — 显示服务详细信息和服务条目。

运行show threat-detection 服务命令以显示所有已启用威胁检测服务的统计信息。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

要查看针对远程访问身份验证服务跟踪的潜在攻击者的更多详细信息，请运行show threat-detection service <service> entries命令。

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source               Interface            Count          Age         Hold-down
--- -------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
```

```
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

要查看特定威胁检测远程访问VPN服务的一般统计信息和详细信息，请运行show threat-detection service <service> details命令。

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

注意：这些条目仅显示威胁检测服务所跟踪的IP地址。如果IP地址满足要避开的条件，则阻止计数增加，并且IP地址不再显示为条目。

此外，您可以监控VPN服务应用的分流器，并使用以下命令删除单个IP地址或所有IP地址的分流器：

- show shun [ip_address]

显示被避开的主机，包括通过VPN服务的威胁检测自动避开的主机，或使用shun命令手动避开的主机。您可以选择将视图限制为指定的IP地址。

- no shun ip_address [interface if_name]

删除应用于指定IP地址的躲避。

如果一个IP地址在多个接口上被避开并且没有提到特定的接口，则该命令仅从一个接口删除回避。此接口的选择取决于对规避的IP地址的路由查找。要从其他接口删除避开设置，必须明确指定接口。

- clear shun

从所有IP地址和所有接口删除回避。

注意：VPN服务的威胁检测避开的IP地址不会出现在show threat-detection shun命令中，该命令仅适用于扫描威胁检测。

要阅读与远程访问VPN的威胁检测服务相关的每个命令输出和可用系统日志消息的所有详细信息，请参阅Cisco Secure Firewall ASA Firewall CLI Configuration Guide， 9.20。章节：威胁检测文档。

相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。联系时需要提供有效的支持合同：思科全球支持联系信息
- 您还可以在这里访问Cisco VPN Community。

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）。