ASA 8.3 及更高版本：使用 MPF 设置 SSH/Telnet/HTTP 连接超时的配置示例

目录

简介

本文档为使用 8.3(1) 及更高版本软件的思科自适应安全设备 (ASA) 提供一个超时的配置示例，此超时配置特定于 SSH/Telnet/HTTP 等特定应用，而非适用于所有应用。此配置示例使用 7.0 版本的思科自适应安全设备 (ASA) 中引入的模块化策略框架 (MPF)。有关详细信息，请参阅使用模块化策略框架。

在此配置示例中，思科 ASA 配置为允许工作站 (10.77.241.129) 通过 Telnet/SSH/HTTP 连接到路由器后部的远程服务器 (10.1.1.1)。还配置了单独的 Telnet/SSH/HTTP 数据流连接超时。所有其他 TCP 流量继续使用与 **timeout conn 1:00:00** 关联的正常连接超时值。

有关使用 8.2 及以前版本软件的思科 ASA 上的相同配置，请参阅 PIX/ASA 7.x 及更高版本 /FWSM：使用 MPF 设置 SSH/Telnet/HTTP 连接超时的配置示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息以采用 Adaptive Security Device Manager (ASDM) 6.3 的思科 ASA 安全设备软件版本 8.3(1) 为基础。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置

本文档使用以下配置：

- CLI 配置
- ASDM 配置

注意： 这些 CLI 和 ASDM 配置适用于防火墙服务模块 (FWSM)。

CLI 配置

ASA 8.3(1) 配置

```
ASA Version 8.3(1)
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 1mZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
ip address 10.77.241.142 255.255.255.0
```

```
boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

!--- Creates an object called DM_INLINE_TCP_1. This
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
port-object eq www port-object eq ssh port-object eq
telnet access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover no
asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound access-group 101 in
interface outside route outside 0.0.0.0 0.0.0.0
192.168.200.2 1 timeout xlate 3:00:00 !--- The default
connection timeout value of one hour is applicable to !-
-- all other TCP applications. timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute timeout tcp-proxy-
reassembly 0:01:00 no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh timeout 5 console timeout 0 ! !--- Define the
class map Cisco-class in order !--- to classify
Telnet/ssh/http traffic when you use Modular Policy
Framework !--- to configure a security feature. !---
Assign the parameters to be matched by class map. class-
map Cisco-class match access-list outside_mpc class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !-
-- Use the pre-defined class map Cisco-class in the
policy map. policy-map Cisco-policy !--- Set the
connection timeout under the class mode where !--- the
idle TCP (Telnet/ssh/http) connection is disconnected.
!--- There is a set value of ten minutes in this
example. !--- The minimum possible value is five
minutes. class Cisco-class set connection timeout idle
0:10:00 reset ! ! service-policy global_policy global !-
-- Apply the policy-map Cisco-policy on the interface.
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command. service-policy Cisco-policy interface outside
end
```

ASDM 配置

请完成以下步骤，以便使用 ASDM 为 Telnet、SSH 和 HTTP 流量设置 TCP 连接超时，如下显示。

注意： 请参阅允许 ASDM 的 HTTPS 访问了解基本设置，以通过 ASDM 访问 PIX/ASA。

1. 选择 **Configuration > Firewall > Service Policy Rules** ，然后点按 **Add**，以便配置服务策略规则，如下所示。
2. 从 **Add Service Policy Rule Wizard - Service Policy** 窗口，选择 **Create a Service Policy and Apply To** 下面的 **Interface** 旁边的单选按钮。现在请从下拉列表中选择所需的接口并且提供**策**

略名称。此示例中使用的策略名称是 Cisco-policy。然后单击 Next。
3. 创建类映射名称 Cisco-class 并在 Traffic Match Criteria 中选中 Source and Destination IP address (uses ACL) 复选框。然后单击 Next。
4. 从 Add Service Policy Rule Wizard - Traffic Match - Source and Destnation Address 窗口，选择 Match 提供所示的源地址和目标地址。点击 Service 旁边的下拉按钮，选择所需的服务。
5. 选择所需的服务，例如 telnet、ssh 和 http。然后，单击OK。
6. 配置超时。单击 Next。
7. 选择 Connection Settings，以便将 TCP 连接超时设置为 10分钟。此外，请选中 Send reset to TCP endpoints before timeout 复选框。单击 完成。
8. 点击 Apply，以便将此配置应用于安全设备。这样就完成了配置。

初期超时

初期连接是半打开的连接，例如，尚未为其完成三方握手的连接。初期连接定义为 ASA 上的 SYN 超时。默认情况下，ASA 上的 SYN 超时是 30 秒。以下是初期超时的配置方法：

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

故障排除

如果发现连接超时对 MPF 无效，请检查 TCP 启动连接。造成该问题的原因可能是源 IP 地址与目标 IP 地址颠倒，或者是访问列表中错误配置的 IP 地址与 MPF 中的不匹配，无法为应用设置新超时值或更改默认超时值。按照连接启动创建访问控制列表条目（源和目标），以使用 MPF 设置连接超时。

相关信息

- Cisco 自适应安全设备管理器
- Cisco ASA 5500 系列自适应安全设备
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems