【MVS】F5 BIG-IP如何限制客户端IP地址对Web界面的访问?

设备管理 **胡伟** 4天前 发表

问题描述

【MVS】F5 BIG-IP如何限制客户端IP地址对Web界面的访问?

解决方法

1， 限制特定地址对带外管理口的访问来防止漏洞利用

l 后台ssh进入tmos视图

[root@bigip1:ModuleNotLicensed::Active:Standalone] config # **tmsh**

root@(bigip1)(cfg-sync Standalone)(ModuleNotLicensed::Active)(/Common)(tmos)#

l 查看当前httpd允许访问地址段

root@(bigip1)(cfg-sync Standalone)(ModuleNotLicensed::Active)(/Common)(tmos)# **list sys httpd allow**

sys httpd {

allow { All }

}

l 修改当前httpd允许访问地址段，这里只允许100.0.0.0/255.255.255.0地址段访问管理口https Web界面

root@(bigip1)(cfg-sync Standalone)(ModuleNotLicensed::Active)(/Common)(tmos)# **modify sys httpd allow replace-all-with { 100.0.0.0/255.255.255.0 }**

l 查看核对修改后的配置

root@(bigip1)(cfg-sync Standalone)(ModuleNotLicensed::Active)(/Common)(tmos)# **list sys httpd allow**

\sys httpd {

allow { 100.0.0.0/255.255.255.0 }

l 保存配置

root@(bigip1)(cfg-sync Standalone)(ModuleNotLicensed::Active)(/Common)(tmos)# **save sys config**

Saving running configuration...

/config/bigip.conf

/config/bigip_base.conf

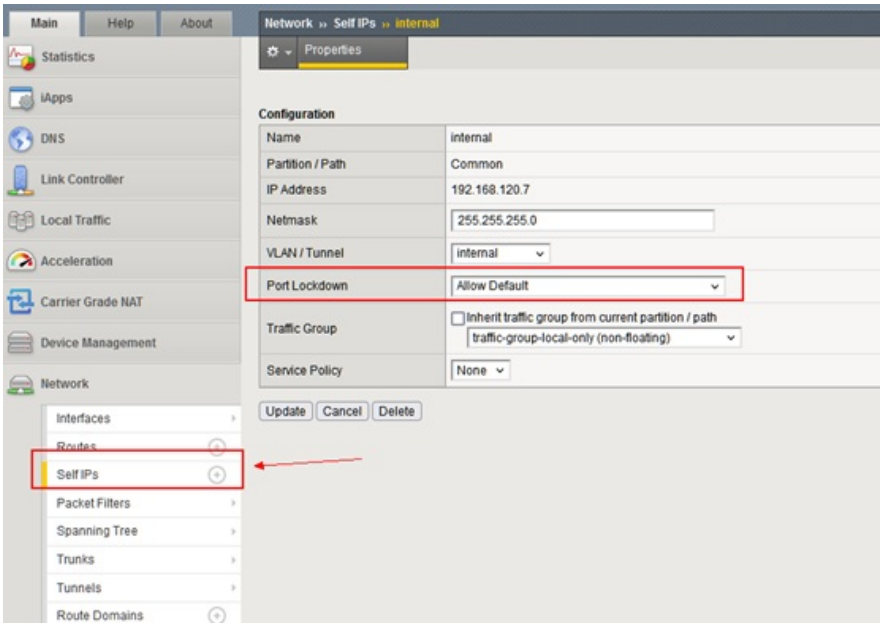
/config/bigip_user.conf

l 结果验证（100.0.0.0/255.255.255.0地址段访问管理口Web被禁止）

2， 限制对业务口TCP 443端口的访问

You can block all access to the Configuration utility of your BIG-IP system using self IP addresses . To do so, you can change the **Port Lockdown** setting to **Allow None** for each self IP address on the system. If you must open any ports, you should use the **Allow Custom** option, taking care to block access to the Configuration utility. By default, the Configuration utility listens on TCP port 443. If you modified the default port, ensure that you block access to the alternate port you configured.

通过使用self IP地址来阻止所有对BIG-IP系统配置Configuration utility的访问。要实现这一点，可以将每个自IP地址的端口锁定（Port Lockdown）设置更改为“允许无”（Allow None）。如果必须打开任何端口，应使用“自定义允许”（Allow Custom）选项，并小心阻止对配置Configuration utility的访问。默认情况下，配置Configuration utility侦听TCP端口443。如果修改了默认端口，请确保阻止对所配置的备用端口的访问。 HA接口可不用配置限制。


Main
Help
About
Statistics
iApps
DNS
Link Controller
Local Traffic
Acceleration
Carrier Grade NAT
Device Management
Network
Interfaces
Routes
Self IPs
Packet Filters
Spanning Tree
Trunks
Tunnels
Route Domains
Network » Self IPs » internal
Properties
Configuration
Name
internal
Partition / Path
Common
IP Address
192.168.120.7
Netmask
255.255.255.0
VLAN / Tunnel
internal
Port Lockdown
Allow Default
Traffic Group
Inherit traffic group from current partition / path
traffic-group-local-only (non-floating)
Service Policy
None
Update
Cancel
Delete