V7虚拟防火墙（Context）命令行配置举例

目录

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等。

1.2 Context配置限制

1.2.1 配置Context前请阅读下表查询所购买的设备是否支持Context?

型号	特性	描述
F5010/F5020/F5030/F5030-6GW/F5040/F5060/F5080/F5000-M/F5000-S/F5000-C	Context	支持
F1005/F1010/F1020/F1030/F1050/F1060/F1070/F1080/F1070-GM		**F1005/F1010：不支持** F1020/F1030/F1050/F1060/F1070/F1080/F1070-GM：支持
F1000-AK108/AK109/AK110/AK115/AK120/AK125/AK130/AK135/AK140/AK145/AK150/AK155/AK160/AK165/AK170/AK175/AK180/AK185/AK710/AK711		**F1000-AK108/AK109/AK110/AK115/AK120/AK125/AK710：不支持** F1000-AK130/AK135/AK140/AK145/AK150/AK155/AK160/AK165/AK1

		70/AK175/AK180/AK185/AK711：支持
F1000-GM-AK370/F1000-GM-AK380		支持
LSU3FWCEA0/LSUM1FWCEAB0/LSX1FWCEA1		支持
LSXM1FWDF1/LSUM1FWDEC0/IM-NGFWX-IV/LSQM1FWDSC0/LSWM1FWD0/LSPM6FWD		支持

1.2.2 配置限制

1. 分配VLAN时的注意事项

对于共享VLAN，请先在缺省Context内创建VLAN，再通过allocate vlan命令将指定VLAN分配给指定的Context使用。

(1)VLAN 1不能被共享。

(2)端口的缺省VLAN不能被共享。

(3)已经创建了VLAN接口的VLAN不能被共享。

2. 分配接口时的注意事项

(1)有些接口可以创建子接口，这样的接口我们称为父接口。分配父接口与子接口时：

不能将子接口独占分配给Context。

如果子接口已经被分配，则不能再分配其父接口。

如果父接口已经被分配，则不能再分配其子接口。

(2)分配聚合接口与成员接口时：

聚合接口只能共享分配给Context。

不能将成员接口共享分配给Context。

(3)如果接口已经被共享分配，则不能再独占分配。需将共享分配配置取消后，才能独占分配。

(4)不允许独占分配逻辑接口。

(5)禁止将IRF物理端口分配给自定义Context。

(6)当三层物理子接口与聚合子接口作为冗余口的成员端口时，禁止把其主接口共享给自定义Context。

1.3 配置需求及实现的效果

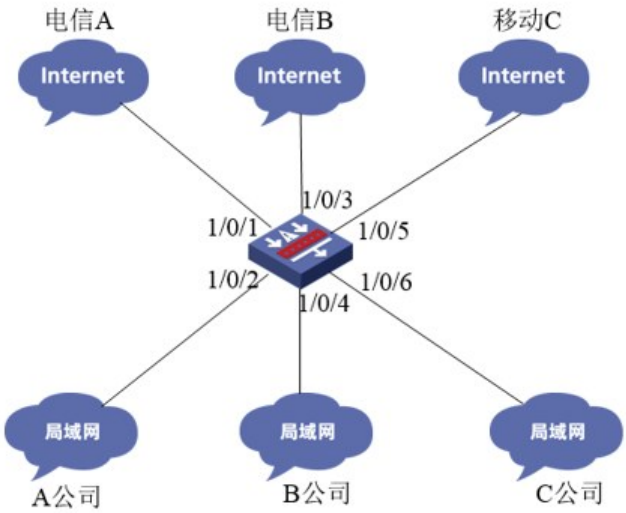
某写字楼有三家公司目前需要部署一台防火墙逻辑上分成三台独立的防火墙，以下为配置需求：

1、A公司用户多、业务复杂，需要为A公司分配较大的内存空间及CPU资源；

2、B公司使用缺省的CPU及内存资源；

3、C公司规模较小，上网流量小，因此分配较低的CPU资源；

2 组网图



3 配置步骤

3.1 A公司虚拟防火墙配置

3.1.1 在根防火墙上创建名称为Company_A的虚拟防火墙

<H3C>system-view

[H3C]context Company_A

[H3C-context-2-Company_A]description Company_A

3.1.2 将Company_A的虚拟防火墙CPU权重设置为8、内存使用上限设置为60%并启动虚拟防火墙

[H3C-context-2-Company_A]limit-resource memory slot 1 cpu 0 ratio 60

[H3C-context-2-Company_A]limit-resource cpu weight 8

[H3C-context-2-Company_A]context start

It will take some time to start the context...

Context started successfully.

3.1.3 配置将接口GigabitEthernet1/0/1和GigabitEthernet1/0/2分配给Context Company_A。

[H3C-context-2-Company_A]allocate interface gigabitethernet 1/0/1 gigabitethernet 1/0/2

Configuration of the interfaces will be lost. Continue? [Y/N]:Y

[H3C-context-2-Company_A]quit

3.1.4 进入Context Company_A的虚拟防火墙配置接口IP地址、路由及NAT地址转换。

[H3C]switchto context Company_A

<H3C>system-view

[H3C]sysname Company_A

[Company_A]interface GigabitEthernet 1/0/1

[Company_A-GigabitEthernet1/0/1]ip address 198.76.28.2 255.255.255.252

[Company_A-GigabitEthernet1/0/1]nat outbound

[Company_A-GigabitEthernet1/0/1]quit

[Company_A]interface GigabitEthernet 1/0/2

[Company_A-GigabitEthernet1/0/2]ip address 172.16.100.1 255.255.255.0

[Company_A-GigabitEthernet1/0/2]quit

[Company_A]ip route-static 0.0.0.0 0 198.76.28.1

3.1.5 进入Context Company_A的虚拟防火墙配置外网与内网的安全域并放通安全策略。

[Company_A]security-zone name untrust

[Company_A-security-zone-Untrust]import interface GigabitEthernet 1/0/1

[Company_A-security-zone-Untrust]quit

[Company_A]security-zone name trust

[Company_A-security-zone-Trust]import interface

GigabitEthernet 1/0/2
[Company_A-security-zone-Trust]quit
[Company_A]security-policy ip
[Company_A-security-policy-ip]rule 1 name pass
[Company_A-security-policy-ip-1-pass]source-zone trust
[Company_A-security-policy-ip-1-pass]destination-zone untrust
[Company_A-security-policy-ip-1-pass]destination-zone local
[Company_A-security-policy-ip-1-pass]action pass
[Company_A-security-policy-ip-1-pass]quit
[Company_A]save f

3.2 B公司虚拟防火墙配置

3.2.1 在根防火墙上创建名称为Company_B的虚拟防火墙

<H3C>system-view
[H3C]context Company_B
[H3C-context-3-Company_B]description Company_B

3.2.2 将Company_B的虚拟防火墙CPU、内存使用系统缺省的资源。

[H3C-context-3-Company_B]context start
It will take some time to start the context...
Context started successfully.

3.2.3 配置将接口GigabitEthernet1/0/3和GigabitEthernet1/0/4分配给Context Company_B。

[H3C-context-3-Company_B]allocate interface gigabitethernet 1/0/3 gigabitethernet 1/0/4
Configuration of the interfaces will be lost. Continue? [Y/N]:Y
[H3C-context-3-Company_B]quit

3.2.4 进入Context Company_B的虚拟防火墙配置接口IP地址、路由及NAT地址转换。

[H3C]switchto context Company_B

<H3C>system-view

[H3C]sysname Company_B

[Company_B]interface GigabitEthernet 1/0/3

[Company_B-GigabitEthernet1/0/3ip address 200.1.8.2 255.255.255.252

[Company_B-GigabitEthernet1/0/3nat outbound

[Company_B-GigabitEthernet1/0/3]quit

[Company_B]interface GigabitEthernet 1/0/4

[Company_B-GigabitEthernet1/0/4]ip address 172.16.200.1 255.255.255.0

[Company_B-GigabitEthernet1/0/4]quit

[Company_B]ip route-static 0.0.0.0 0 200.1.8.1

3.2.5 进入Context Company_B的虚拟防火墙配置外网与内网的安全域并放通安全策略。

[Company_B]security-zone name untrust

[Company_B-security-zone-Untrust]import interface GigabitEthernet 1/0/3

[Company_B-security-zone-Untrust]quit

[Company_B]security-zone name trust

[Company_B-security-zone-Trust]import interface GigabitEthernet 1/0/4

[Company_B-security-zone-Trust]quit

[Company_B]security-policy ip

[Company_B-security-policy-ip]rule 1 name pass

[Company_B-security-policy-ip-1-pass]source-zone trust

[Company_B-security-policy-ip-1-pass]destination-zone untrust

[Company_B-security-policy-ip-1-pass]destination-zone local

[Company_B-security-policy-ip-1-pass]action pass

[Company_B-security-policy-ip-1-pass]quit

[Company_B]save f

3.3 C公司虚拟防火墙配置

3.3.1 在根防火墙上创建名称为Company_C的虚拟防火墙

<H3C>system-view

[H3C]context Company_C

[H3C-context-4-Company_C]description Company_C

3.3.2 将Company_C的虚拟防火墙CPU权重设置为2、内存使用上限设置为20%并启动虚拟防火墙。

[H3C-context-4-Company_C]

[H3C-context-4-Company_C]limit-resource memory slot 1 cpu 0 ratio 20

[H3C-context-4-Company_C]limit-resource cpu weight 2

[H3C-context-4-Company_C]context start

It will take some time to start the context...

Context started successfully.

3.3.3 配置将接口GigabitEthernet1/0/5和GigabitEthernet1/0/6分配给Context Company_C。

[H3C-context-4-Company_C]allocate interface gigabitethernet 1/0/5 gigabitethernet 1/0/6

Configuration of the interfaces will be lost. Continue? [Y/N]:Y

[H3C-context-4-Company_C]quit

3.3.4 进入Context Company_C的虚拟防火墙配置接口IP地址、路由及NAT地址转换。

[H3C]switchto context Company_C

<H3C>system-view

[H3C]sysname Company_C

[Company_C]interface GigabitEthernet 1/0/5

[Company_C-GigabitEthernet1/0/5]ip address 100.100.99.2

255.255.255.252

[Company_C-GigabitEthernet1/0/5]nat outbound

[Company_C-GigabitEthernet1/0/5]quit

[Company_C-interface GigabitEthernet 1/0/6

[Company_C-GigabitEthernet1/0/6]ip address 172.16.300.1 255.255.255.0

[Company_C-GigabitEthernet1/0/6]quit

[Company_C]ip route-static 0.0.0.0 0 100.100.99.1

3.3.5 进入Context Company_C的虚拟防火墙配置外网与内网的安全域并放通安全策略。

[Company_C]security-zone name untrust

[Company_C-security-zone-Untrust]import interface GigabitEthernet 1/0/5

[Company_C-security-zone-Untrust]quit

[Company_C]security-zone name trust

[Company_C-security-zone-Trust]import interface GigabitEthernet 1/0/6

[Company_C-security-zone-Trust]quit

[Company_C]security-policy ip

[Company_C-security-policy-ip]rule 1 name pass

[Company_C-security-policy-ip-1-pass]source-zone trust

[Company_C-security-policy-ip-1-pass]destination-zone untrust

[Company_C-security-policy-ip-1-pass]destination-zone local

[Company_C-security-policy-ip-1-pass]action pass

[Company_C-security-policy-ip-1-pass]quit

[Company_C]save f

3.3.6 保存配置

激活前需要保存根墙，以免重启后配置丢失。

[Company_C]quit

[H3C]save f

4 配置注意事项

4.1.1 关于防火墙WEB界面登录问题

1. 虚拟防火墙默认情况下未开启WEB登录界面，请使用下面命令开启；

以Company_A的虚拟防火墙举例：

[H3C]switchto context Company_A

[Company_A]ip https enable

[Company_A]user-interface vty 0 63

[Company_A-line-vty0-63]authentication-mode scheme

[Company_A]local-user admin

[Company_A-luser-manage-admin]password simple admin

[Company_A-luser-manage-admin]authorization-attribute user-role level-15

[Company_A-luser-manage-admin]service-type https

[Company_A-luser-manage-admin]quit

[Company_A]save f

完成上述配置后请使用172.16.100.1登录设备，前面案例中已经放通trust到local区域的安全策略，如果需要外网访问防火墙，需要放通untrust到local区域的安全策略。