[2012-5-7]H3C Comware V5平台防火墙维护类常见问题FAQ

金山 2012-05-07 发表

H3C Comware V5平台防火墙维护类常见问题FAQ

Q：H3C Comware V5平台防火墙的域间策略加速和ACL加速功能如何使用?

A：部分V5平台高端型号产品支持域间策略加速和ACL加速功能。以域间策略加速为例，当相同源、目的安全区域之间的域间策略数量非常多时（通常指规则数超过1000条以上），防火墙软件在进行域间策略匹配判断时处理速度会受到影响。为提高策略匹配速度，可以在配置完成相同源、目的区域之间的全部域间策略后，使能该源、目的安全区域之间的域间策略加速功能，加快防火墙软件处理速度。域间策略加速功能开启后，不允许再对该源、目的安全区域相应的域间策略进行修改操作，否则会造成加速功能失败、策略匹配功能异常，只能通过关闭策略加速功能恢复。ACL加速与域间策略加速功能原理基本相同。综上，不建议使用域间策略加速和ACL加速功能。如果因测试或特殊应用场景原因必须启用，则必须注意在启用该功能后一旦需要修改域间策略或ACL规则，应先停止加速，然后修改配置，最后再重新使能加速功能。

Q：H3C Comware V5平台防火墙会话表老化时间应如何调整?

A：以TCP协议会话为例，V5平台防火墙默认配置SYN_SENT和SYN_RCV状态为30秒、FIN_WAIT状态为30秒、ESTABLISHED状态为3600秒。在防火墙实际运维部署过程中，如果将会话表各状态老化时间调节得比默认值更短，则防火墙上没有实际业务报文交互的会话表项可以在更短的时间内由于计时器超时而清除，达到减少防火墙并发连接数的目的；但如果将会话表项老化时间调整过短，容易出现上层应用的数据报文交互还没有完成，防火墙上会话表项却因为计时器超时而老化，后续的数据报文由于没有会话而被防火墙丢弃。反之如果将会话表项老化时间调整得更长，那么当某条会话表项不再交互报文，或由于上层应用出现异常不能正常关闭时，这条表项就需要等待更长的时间才能因计时器超时而清除。

综上，在通常情况下不建议修改默认的防火墙会话表老化时间参数。如果防火墙在运行过程中并发连接数长时间持续较高，可以适当调低各协议各状态的老化时间，以降低并发连接数。

Q：客户某应用基于TCP连接，但在业务交互过程中可能会出现在客户端和服务器之间会话长时间没有报文交互，但V5防火墙TCP协议EST状态老化时间只有1小时，应该如何解决?

A：针对这种情况，如果简单地将TCP协议EST状态会话老化时间改为较长时间，会造成防火墙上创建的所有会话的老化时间都比较长，进而大大增加防火墙并发会话数，因此不建议使用这种方式。在V5平台防火墙上，支持会话长连接功能，可以预先配置一条描述需要设置较长老化时间TCP流的ACL，然后基于这个ACL配置长连接并单独设置老化时间，这样既可以保证个别业务应用的使用，又避免防火墙上出现大量长时间不能老化的TCP会话。

Q：Comware V5平台防火墙“单向流检测”功能是怎样的？哪些场景需要使用?

A：通常情况下，Comware V5平台防火墙在处理网络流量时，严格按照协议及域间策略检查经过设备的报文，对于合法报文，可以正常建立防火墙会话表项并转发，对于异常报文及不符合域间策略的报文则丢弃处理。

以TCP协议为例，防火墙上默认存在Trust区域至Untrust区域允许的策略，Trust区域客户端首先发起连接，向处于Untrust区域的服务器建立TCP三次握手连接。防火墙从正向收到SYN，反向收到SYN+ACK，正向收到ACK报文后，创建一条TCP EST状态的会话表项。但如果因组网原因，例如V5防火墙和另一台路由器共同部署在网络出口，上行流量通过V5防火墙转发，下行流量通过路由器转发，那么在V5防火墙上，就仅能收到SYN报文和ACK报文，SYN+ACK报文不经过防火墙。如此在V5防火墙上是无法创建会话表项的，后续业务报文也不能正常转发处理。UDP、ICMP协议的情况与前述TCP协议类似。

当我们在V5平台防火墙上使能“单向流检测”后，在域间策略允许的前提下，以TCP协议为例，防火墙从正向接收到SYN报文和ACK报文，或者从反向接收到SYN+ACK报文，都可以直接创建一条EST状态的TCP会话表项。这样该条会话的后续报文就可以转发了。UDP、ICMP协议使能该特性后原理与TCP协议相似。

除防火墙和路由器组网且来回路径不一致的环境外，在H3C V5平台防火墙与其他友商防火墙或路由交换设备混合组网且来回路径不一致环境、或者其他的只有单向报文经过防火墙的特殊组网环境中，都可以通过开启“单向流检测”使防火墙可以正常创建会话表项并转发业务报文。由于“单向流检测”功能开启后，防火墙对会话表项创建条件的检查相对较弱，因此不建议在普通组网环境中开启此功能，避免削弱防火墙的安全性。

Q：H3C Comware V5平台防火墙上默认开启的虚拟分片重组功能是怎样的?

A：V5防火墙支持虚拟分片重组功能，可以对网络中的三层IP分片报文执行缓存、重组、排序转发等功能。当防火墙从网络中收到三层IP分片报文后，会将分片报文根据配置参数缓存在本地，等待后续分片全部到达。如果后续分片没有发送至防火墙，或分片报文有错误，则防火墙可以丢弃未能成功重组的报文，并上报分片报文攻击日志。如果所有分片均在规定时间内到达防火墙，且防火墙重组全部分片成功，那么防火墙可以实现将乱序的分片报文重新按正确的顺序转发出去，从则为上层协议或其他

设备带来好处。V5防火墙在各安全区域上默认支持64个分片队列，即同一时刻最多可以同时对64个分片报文执行重组，当网络中的分片报文较多时，可以将分片队列参数调整至最大值1024。

Q：H3C Comware V5平台防火墙支持的虚拟防火墙功能应该如何部署应用?
A：因组网应用需求，有时需要将一台物理防火墙虚拟成多台防火墙部署在网络中，此时便可以使用虚拟防火墙功能。一台物理防火墙虚拟为多台逻辑防火墙后，各个虚拟防火墙支持相互独立的配置管理，可以分别进行安全区域、域间策略的配置。如果各个虚拟防火墙之间需要互访，可以通过配置共享安全区域实现。配置虚拟防火墙以后，各个虚墙还是共享路由交换平面的，如果希望将路由交换也完全隔离，则可以通过在防火墙上为每个虚拟防火墙创建和绑定VPN实例来实现。如果虚拟防火墙是二层模式的，则可以通过将涉及的VLAN分配给相应的虚拟防火墙来实现。虚拟防火墙部署完成后，还应该注意所有虚拟报文墙的会话表与主墙是共享内存空间的。如果还配置了VPN实例，应注意有很多配置都需要增加相应VPN实例名，否则涉及的配置命令无法正常生效。

Q：H3C Comware V5平台防火墙双机热备功能如何实现，在何种情况下需要启用“支持非对称路径”功能?
A：为实现两台V5防火墙互备组网中，业务流量因故出现主备倒换后，实现平滑切换的需求。要求两台防火墙必须实现将本墙创建的防火墙会话表项，实时同步备份至另一台防火墙，使得当业务流量切换至另一台防火墙时仍然能够转发每个会话的后续报文。反之如果不备份防火墙会话表项，那么当业务流量发生倒换，每条会话的后续报文转到另一台防火墙处理后，由于备防火墙收到报文后查询会话列表不能匹配，且报文也不是会话首包，也不满足域间策略创建会话的条件，那么这些报文会被备份防火墙丢弃，两台防火墙之间无法实现热备效果。
使能双机热备功能后，两台V5防火墙形成互备关系，进入同步运行状态。当网络流量在一台防火墙上形成稳定状态的会话表项后（TCP协议ESTABLISHED状态、UDP协议READY状态、ICMP协议CLOSED状态、RAWIP协议READY状态），创建会话的防火墙将会把这条会话表项信息通过HA线同步至另一台防火墙。一旦业务流量发生切换，另一台防火墙已经有了相应的会话表项，因此在收到每条会话的后续报文时仍然可以正常处理和转发。
在部署防火墙双机热备后如果网络流量走向来回路径不一致，比如上行方向通过两台互备防火墙中的A墙转发，下行方向通过B墙转发。当从内网访问外网时，TCP协议首包SYN报文由A墙处理，创建SYN_SENT状态的会话，由于还没有进入稳态，不同步至B墙；服务器响应报文SYN+ACK报文返回时由B墙处理，由于没有会话表项，不符合TCP协议状态机，也不满足域间策略，B墙会直接丢弃该报文，此时业务不通。开启“支持非对称路径”功能后，防火墙在维护会话表的过程中，会将除本地收发的会话表项外其余全部会话发生创建、更新、删除事件时同步其状态至另一台防火墙。再次按前述组网条件为例考虑，当上行流量通过A墙处理，创建TCP SYN_SENT状态的会话后，虽然会话还未进入稳定状态，但使能“支持非对称路径”特性后，A墙将该这条会话表项同步至B墙处理。B墙收到返回的SYN+ACK报文后，由于已经有的相应的SYN_SENT状态的会话，因此转发报文后，将这条会话表项更新至SYN_REV状态，状态更新后的会话表项再次同步给A墙，A墙后续再收到ACK报文，会话表再次更新至EST状态并同步更新至B墙。从上面的处理过程中，可以发现来回路径不一致的组网防火墙双机也可以满足。最后需要说明的是，开启“支持非对称路径”后，由于防火墙进行的与备份会话有关的操作更多了，因此对CPU性能的消耗要比不启用该特性时更多。

Q：H3C Comware V5平台防火墙双机热备组网，防火墙运行在二层模式和三层模式各有哪些注意事项?
A：防火墙运行在二层模式时，如果是盒式防火墙，正常部署即可；如果是插卡式防火墙，由于二层部署需做跨VLAN二层转发，这是一种很特殊的组网方式，相同于把两个VLAN连通成一个广播域，因此比较容易出现二层广播环路，不做推荐。
防火墙运行在三层模式时，无论盒式或插卡式防火墙，都不建议在两台防火墙之间再部署三层互联，即在任何情况下都不建议同一条会话的报文同时经过形成双机热备关系的两台防火墙进行转发。一方面报文两次经过防火墙转发，在两台防火墙上很容易出现会话表记录的源、目的安全区域和设备实际接收到报文的源、目的安全区域不符；另一方面业务流量经过两台防火墙其中一台即可完成域间策略匹配，实现各安全区域之间的互访控制，两次经过防火墙转发会引入不必要的处理时延。

Q：H3C Comware V5平台防火墙双机热备组网，进行NAT配置时有哪些注意事项?
A：V5平台防火墙双机热备组网后，进行NAT配置时应注意关联VRRP，保证防火墙上下游设备可以正常学习到NAT相关地址的ARP表项。以NAT Outbound为例，两台V5防火墙使用相同的地址池执行NAT转换，内网发起NAT会话后，对端设备返回报文时需查询转换后IP地址对应的MAC地址。由于两台防火墙上配置了相同的NAT命令，所以两台防火墙都响应ARP查询便会引起ARP学习混乱。通过在防火墙上配置一组VRRP，然后利用VRRP的状态代表防火墙的主备状态，VRRP状态为Master的防火墙负责响应上下游设备的ARP查询报文，从而解决了两台防火墙同时响应ARP报文的混乱问题。同理，如果两台防火墙的NAT Static、NAT Server命令为实现互为备份，那么也应该通过关联VRRP，使两台防火墙中只有一台会响应上下游设备的ARP查询报文。
在NAT Outbound配置关系的地址池配置中，还包含一个高、低优先级概念。在配置时应注意，如果两台防火墙使用包含相同地址的地址池，那么在两台防火墙上相同地址池的优先级不能相同。如果形成热备的防火墙是主备关系，正常运行时流量全部在A墙上，那么可以将A墙的地址池配置为非低优先级，B墙地址池配置为低优先级；如果形成热备的防火墙是负载分担关系，正常运行时流量在两台防火墙

上都会执行NAT Outbound，那么建议将公网地址池分为两部分，前一部分在A墙上配置为非低优先级，后一部分配置为低优先级，反之在B墙上前一部分配置为低优先级，后一部分配置为非低优先级。这样配置才能保证双机业务正常运行，当其中一台防火墙出现故障后NAT业务流量可以平滑切换至另一台防火墙。
在实施有VRF（VPN实例）的组网中，配置NAT命令时应注意关联相应的VPN实例。比如NAT Server命令，不论是公网侧还是私网侧，在配置命令各参数时都需要根据实现组网情况配置VPN实例关联，否则无法正常实现NAT功能。

Q：H3C Comware V5平台防火墙ALG模块有哪些功能，部署时有哪些注意事项?
A：V5平台防火墙ALG模块的主要功能是配合NAT提供应用层地址信息转换功能，还可以配合域间策略模块创建关联表会话，以便多通道应用正常交互。比如针对FTP应用，在NAT前后由ALG执行TCP报文头部以上的地址、端口信息的转换，以及在FTP主动模式下，放开服务器向客户端主动发起的FTP数据连接。
在防火墙运行过程中，由于匹配ALG创建的关联表的会话流量不能快速转发，会降低防火墙吞吐性能，因此建议如果不使用ALG相应的功能可以将其禁用。在防火墙新版本软件中，默认配置下仅使能FTP协议ALG功能，而老版本防火墙软件中则是默认全部开启的。

Q：H3C Comware V5平台防火墙Userlog日志包含哪些内容，部署时有哪些注意事项?
A：V5平台防火墙支持Userlog日志功能。从名称看，Userlog日志与系统日志即Syslog相对，记录了除防火墙系统日志以外的其他信息，目前主要包含一种日志即会话日志，也称NAT日志。Userlog日志分V1、V3两种格式，如果希望记录某条会话在地址转换前和转换后的地址，必须使用V3格式进行输出。事实上无论防火墙上是否配置有NAT都可以输出Userlog日志。Userlog日志通常需要输出至一台日志主机查看，例如H3C SecCenter FW Manager，防火墙向SecCenter的UDP 30017端口以二进制流形式的输出日志，由SecCenter FWM接收后通过Web界面提供显示和查询功能；防火墙还支持通过信息中心以Syslog格式向日志主机输出，这样即使是普通的Syslog日志主机也能接收查看，但这种输出方式对防火墙CPU性能消耗较大，通常不建议采用这种部署方式。除了配置Userlog输出格式和具体的日志主机地址、端口等参数外，注意还要配置日志输出策略，必须配置需要输出日志的会话源安全区域、目的安全区域、其他输出参数等，防火墙才会真正产生Userlog日志并输出至日志主机。