**信息安全评估竞赛考核方案**

一、竞赛考核知识内容

1、园区网IP规划设计的基本原则与实现方法；

2、园区网信息安全规划设计的基本原则与实现方法；

3、三层虚拟化交换机中信息安全相关的配置操作；

4、防火墙中信息安全相关的配置操作；

5、WEB应用防火墙中信息安全相关的配置操作；

6、网络日志系统中信息安全相关的配置操作；

7、无线交换机与无线接入点中信息安全相关的配置操作；

二、考核内容

完成一个企业园区网的信息安全相关的规划设计，并完成相关安全设备的配置与调试工作。

1、整个网络的组网拓扑如下：



2、整个网络的安全设备及具体配置基本参数如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **管理地址** | **默认管理接口** | **用户名** | **密码** |
| 防火墙DCFW | <http://192.168.1.1> | ETH0 | admin | admin |
| 网络日志系统DCBI | https://192.168.5.254 | ETH0 | admin | 123456 |
| WEB应用防火墙WAF | https://192.168.45.1 | ETH5 | admin | admin123 |
| 三层交换机DCRS | - | Console | - | - |
| 无线交换机DCWS | - | Console | - | - |
| 堡垒服务器DCST | - | - |  |
| 备注 | 所有设备的默认管理接口、管理IP地址不允许修改。 |

3、整个网络的IP规划：

|  |  |  |  |
| --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **对端设备** |
| 防火墙DCFW | ETH0/2 | 10.0.0.1/30 | DCRS |
| ETH0/1 | 10.1.4.78/24 | PC3（10.1.4.77） |
| L2TP | 192.168.10.1/24可用IP数量为20 | L2TP地址池 |
| ETH0/3 | 10.0.0.10/30 | Netlog |
| 无线控制器DCWS | VLAN 1002ETH1/0/1 | 10.0.0.6/30 | DCRS |
| ETH1/0/2 |  | AP |
| 管理VLANVLAN 100 | 192.168.100.254/24 |  |
| VLAN 101ETH1/0/11-24 | 192.168.101.1/24 |  |
| WEB应用防火墙WAF | ETH2 | 172.16.100.2/24 | DCST |
| ETH3 | DCRS |
| 三层交换机DCRS | VLAN 1001ETH1/0/2 | 10.0.0.2/30 | DCFW |
| VLAN 1002ETH1/0/1 | 10.0.0.5/30 | DCWS |
| VLAN 10 | 172.16.10.1/24 | 无线2 |
| VLAN 20 | 172.16.20.1/25 | 无线1 |
| 无线管理VLANVLAN 30 | 172.16.30.1/26 |  |
| VLAN 40ETH1/0/6-9 | 192.168.40.1/24 | PC1　 |
| 管理VLANVLAN 100 | 192.168.100.1/24 |  |
| VLAN 200ETH1/0/10-24 | 172.16.100.1/24 | WAF、PC2 |
| 日志服务器Netlog | ETH2 | 10.0.0.9/30 | DCFW |
| ETH3 |  | DCRS(ETH1/0/4) |

三、考核具体要求：

1、任务1：网络平台搭建：根据网络拓扑图所示，完成如下操作任务。

|  |  |
| --- | --- |
| 编号 | 任务需求 |
| 1 | 按照IP地址参数表，对WAF的名称、各接口IP地址进行配置。 |
| 2 | 按照IP地址参数表，对DCRS的名称、各接口IP地址进行配置。 |
| 3 | 按照IP地址参数表，对DCFW的名称、各接口IP地址进行配置。 |
| 4 | 按照IP地址参数表，对DCWS的各接口IP地址进行配置。 |
| 5 | 按照IP地址参数表，对DCBI的名称、各接口IP地址进行配置。 |
| 6 | 按照IP地址参数表，在DCRS交换机上创建相应的VLAN，并将相应接口划入VLAN。 |
| 7 | 采用静态路由的方式，全网络互连。 |
| 8 | 防火墙做必要配置实现内网对外网访问 |

2、任务2：网络安全设备配置与防护

（1） 在DCFW上配置，连接LAN接口开启PING,HTTP,HTTPS，telnet功能，连接Internet接口开启PING、HTTPS功能；连接netlog接口为DMZ区域，合理配置策略，让内网用户能通过网络管理netlog；

（2） DCFW配置 LOG，记录NAT会话， Server IP为172.16.100.10.开启DCFW上snmp服务，Server IP 172.16.100.10 团体字符为public5；

（3） DCFW做相应配置，使用L2TP方式让外网移动办公用户能够实现对内网的访问，用户名密码为dcn2015， VPN地址池参见地址表；合理配置安全策略；

（4） 出于安全考虑，无线用户移动性较强，无线用户访问 Internet是需要采用实名认证，在防火墙上开启Web认证，账号密码为2015web；

（5） 为了合理利用网络出口带宽，需要对内网用户访问Internet进行流量控制，园区总出口带宽为200M，对除无线用户以外的用户限制带宽，每天上午9:00到下午6:00每个IP最大下载速率为2Mbps，上传速率为1Mbps；

（6） DCFW上配置NAT功能，使PC3能够通过Web方式正常管理到AC，端口号使用6665;）合理配置安全策略；

（7） 在DCFW做相关配置要求防火墙能够记录每天9:00-18:00内网用户访问外网的URL，保存在日志服务器；

（8） 配置防火墙Web外发信息控制策略，禁止内网无线用户到所有网站的Web外发信息控制；内网有线用户到外网网站Web外发信息控制，禁止外发关键字“攻击”“病毒”，信任值为1，并记录相关日志。

（9） DCFW做相关配置要求内网用户不能登录QQ和MSN；

（10） DCFW上配置限制内网用户访问www.sohu.com 限制内网用户访问URL中带有sohu关键字的所有网站；

（11） 在DCBI-netlog上配置，设备部署方式为旁路模式，并配置监控接口与管理接口;要求对内网访问Internet全部应用进行记录日志；

（12） 在DCBI-netlog上配置，监控周一至周五9：00-18：00 无线用户所在网段访问的URL中包含sohu的HTTP访问记录，并且邮件发送告警；

（13） 在DCBI上配置，添加内容规则，对于网站访问关键字包含“搜狐”的，记录并邮件报警；

（14） 在DCBI上配置，使DCBI能够通过邮件方式发送告警信息，邮件服务器IP 172.16.100.20，端口号25，账号test5dcn，密码test5，当DCBI磁盘使用率超过90%时发送一次报警；

（15） 在DCBI上配置，将DCBI的日志信息发送到日志服务器，日志服务器IP 172.16.100.10，community名字public3；

（16） 在DCBI上配置，增加非admin账户DCN2015，密码dcbi5555，该账户仅用于用户查询设备的日志信息和统计信息；

（17） DCBI配置应用及应用组“P2P下载”，UDP协议端口号范围40500-42000，在周一至周五9：00-18：00监控LAN中所有用户的“P2P下载”访问记录并告警；

（18） 在WAF上配置，公司内部有一台网站服务器直连到WAF，IP地址是172.16.100.30，端口是8080，并将服务访问日志、Web防护日志、服务监控日志发送至syslog日志服务器，syslog日志服务器IP地址是172.16.100.10，UDP的514端口；

（19） 在公司总部的WAF上配置，将攻击告警、设备状态告警信息通过邮件（发送到DCN@digitalchina.com）及短信方式(发送到13913814949)发送给管理员；

（20） 在公司总部的WAF上配置，禁止公网IP地址（218.5.18.2）访问网站服务器，网站服务器IP地址是172.16.100.30；

（21） 在公司总部的WAF上配置，防止某源IP地址在短时间内发送大量的恶意请求，影响公司网站正常服务。大量请求的确认值是：并发访问超过3000次请求；

（22） 在WAF上配置，开启基于 session cookie的CC防护，最大请求数为3000，超过进行阻止；

（23） DCRS为接入交换机，为终端产生防止MAC地址防洪攻击，请配置端口安全，每个已划分VLAN的端口最多学习到25个MAC地址，发生违规阻止后续违规流量通过，不影响已有流量并产生LOG日志；连接PC1的接口为专用接口，限定只允许PC1的MAC地址可以连接；

（24） 将连接DCFW的双向流量镜像至Netlog进行监控和分析；

（25） 开启防ARP扫描功能，单位时间内端口收到ARP数量超过50便认定是攻击，DOWN掉此端口；

（26） 在公司总部的DCRS上配置端口环路检测（Loopback Detection），防止来自VLAN200接口下的单端口环路，并配置存在环路时的检测时间间隔为30秒，不存在环路时的检测时间间隔为10秒；

（27） 为了控制接入网络PC，需要在交换ETH1/0/10口开启DOT1X认证，配置认证服务器，IP地址是172.16.100.40，radius key是dcn2015；

（28） 交换机开启远程管理，使用SSH方式账号为DCN2015，密码为555555；

（29） VLAN20、VLAN30、VLAN10 用户采用动态获取IP地址方式，DHCP服务器在AC上配置，前十个地址为保留地址，VLAN40用户也动态获取IP，DHCP server为DCFW；

（30） 在交换机上配置，在只允VLAN200用户在上班时间（周-到周五8:00到18:00）内访问VLAN100段IP；

（31） 为拦截、防止非法的MAC地址与IP地址绑定的ARP数据包配置动态arp检测功能，VLAN30用户的ARP阀值为50；

（32） 为了防止VLAN40网段arp欺骗，需要在交换机上开启ip dhcp snooping并在接口下绑定用户；

（33） 在DCRS上配置，配置设备enable密码，密码为dcn2015，并且在登录设备时必须正确输入enable密码才能进入交换机的配置模式；

（34） DCRS上配置，VLAN40的成员接口开启广播风暴抑制功能，参数设置为2500pps；

（35） AP通过option43方式进行正常注册上线,hwtype 值为59,AC地址为管理VLANIP；

（36） 设置SSID DCN2015，VLAN10，加密模式为wpa-personal,其口令为GSdcn2015的；设置SSID dcntest ，VLAN20不进行认证加密,做相应配置隐藏该ssid；

（37） dcntest最多接入20个用户，用户间相互隔离，并对dcntest网络进行流控，上行速率1Mbps，下行速率2Mbps；

（38） 通过配置避免接入终端较多且有大量弱终端时，高速客户端被低速客户端“拖累”，低速客户端不至于长时间得不到传输；

（39） 通过配置防止多AP和AC相连时过多的安全认证连接而消耗CPU资源，检测到AP与AC在10分钟内建立连接5次就不再允许继续连接，两小时后恢复正常；

（40） AC开启Web管理，账号密码为DCN2015；