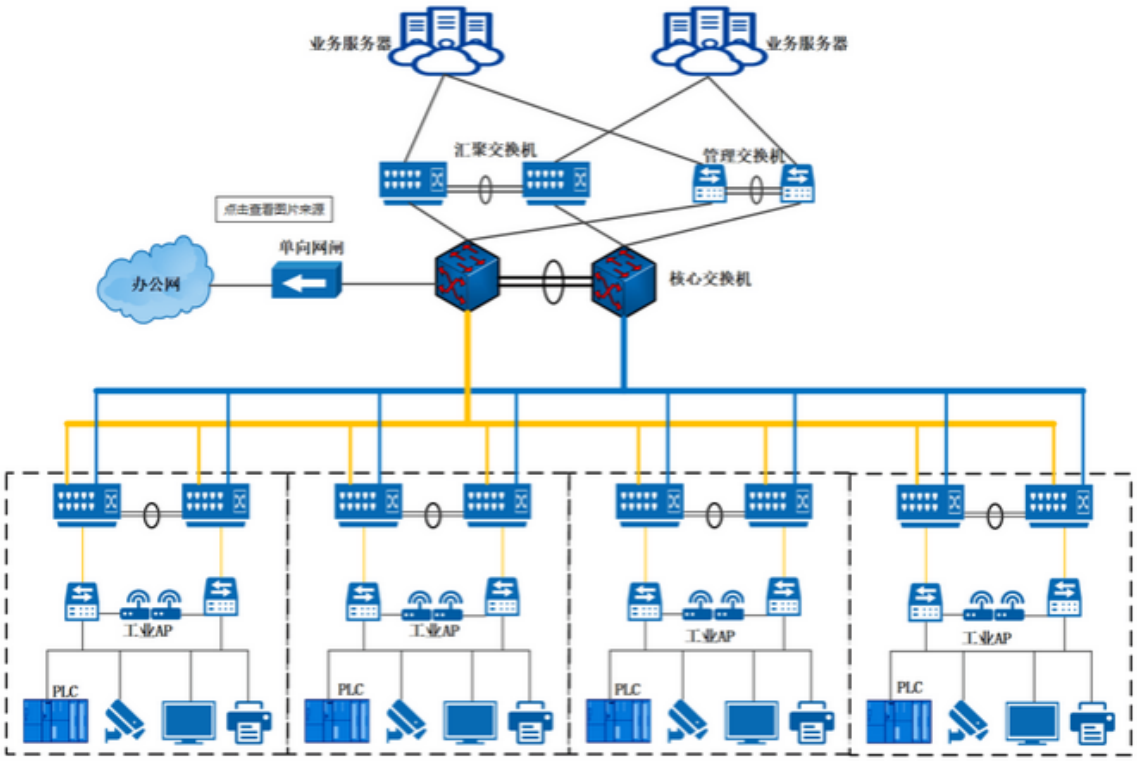
内网隧道代理技术

隧道描述

攻击者通过边界主机进入内网，往往会利用它当跳板进行横向渗透，但现在的内部网络大多部署了很多安全设各，网络结构错综复杂，对于某些系统的访问会受到各种阻挠，这就需要借助代理去突破这些限制，因此面对不同的网络环境对于代理的选择及使用显得格外重要。



隧道的分类

关于隧道的分类大体可以从两个方面进行分类

如果是从流量层分类

1、应用层隧道（DNS SOCKS HTTP SSH）

2、传输层隧道（TCP隧道 UDP隧道）

3、网络层隧道（ICMP隧道 IPv6隧道）

如果从作用上来分类

1、反弹SHELL（nc python bash）

2、端口转发（LCX SSH iptables telnet）

3、端口映射（LCX NPS FRP）

3、正向代理 (EW NSP FRP)

4、反向代理 (EW NSP FRP)

重要概念

端口转发和端口映射

端口转发,有时被称为做隧道,是安全壳(SSH)为网络安全通信使用的一种方法简单来说,端口转发就是将一个端口收到的流量转发到另一个端口。

端口映射是 NAT的一种,功能是把在公网的地址转成私有地址。简单来说,端口映射就是将一个端口映射到另一个端口供其他人使用

Http代理和Socks代理（隧道）

Http代理用的是Http协议，工作在应用层，主要是用来代理浏览器访问网页。

Socks代理用的是Socks协议，工作在会话层，主要用来传递数据包。socks代理又分为Socks4和Sock5，Socks4只支持TCP，而Socks5支持TCP和UDP。

反弹shell介绍

反弹shell（reverse shell），就是控制端监听在某TCP/UDP端口，被控端发起请求到该端口，并将其命令行的输入输出转到控制端。reverse shell与telnet，ssh等标准shell对应，本质上是网络概念的客户端与服务端的角色反转。

正向代理和反向代理

正向是从攻击者电脑主动访问目标机器，例如通过主动访问目标建立Shell是正向Shell。

反向是从目标机器主动连接攻击者电脑，例如通过在目标机器执行操作访问攻击者电脑建立的Shell是反向Shell