

【CSC 公开课】第十八期——思科 AnyConnect 安全接入 问题解答

- ✓ 问题：ASA 上怎么实现 token 的双重认证？
- ✓ 回答：你所说的双认证，是指 token + 静态密码，双认证？ 是针对于 VPN 的拨入认证吗
- ✓ 问题：是的。动态密码+静态密码
- ✓ 回答：常见搭配是与 3a 服务器联动，比如 ACS。动态认证使用 token 与 ACS 来结合，同时，asa 的静态认证使用 secondary authentication
- ✓ 问题：这个 token 是单独的一套系统或软件吗
- ✓ 回答：是的
- ✓ 问题：思科自己有吗？还是必须使用第三方的？
- ✓ 回答：据我所知，思科没有自己的。如有相关深入的咨询，建议咨询相关的思科销售。
- ✓ 问题：好的，非常感谢。
- ✓ 问题：外部用户拨入公司 VPN 后，怎么实现通过公司 ASA 访问公网？（VPN 用户数据达到 ASA 后再访问公网）
- ✓ 回答：按照文档说的，U-turn

- ✓ 问题：token 设备比较靠谱的设备都有哪些？
- ✓ 回答：对于这点思科并没有相关官方推荐，很抱歉
- ✓ 问题：VPN 的 licesen 分哪些？有什么区别？
- ✓ 回答：
http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/prod_brochure0900aecd80402e39.html

- ✓ 问题：anyconnect 客户端上能否隐藏 组选择 的选项？
- ✓ 回答：你说的组选项，若是指拨入界面看到的 group name，那客户端上没有选项去隐藏它
- ✓ 问题：输入用户名和密码后 自动识别所在组
- ✓ 回答：可以使用 profile 来，从 asa 推给客户端，从而实现绑定组。也可以使用直接拨入 group-url，来实现绑定组。

- ✓ 问题：恩是说的 拨入界面看到的 group name, 您的意思是只是输入用户密码后, 无法自动识别属于哪个 group, 是吗?
- ✓ 回答：可以使用 profile 来, 从 asa 推给客户端, 从而实现绑定组。也可以使用直接拨入 group-url, 来实现绑定组
- ✓ 问题：group-url 有没有配置案例啊, 我在官网没有找到相关的案例
- ✓ 回答：
<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html>
- ✓ 问题：DAP 上面设置信息提示, 能否使用中文字符? ASA + Anyconnect 可否审计哪些用户曾经连接 VPN? 能否审计用户通过 Anyconnect 连接 VPN 后访问过一些什么网络资源 (IP add/URL)?
- ✓ 回答：DAP 使用建议都用英文。你这样的审计需求, asa 无法实现。建议使用 3a 服务器。通过 vpn 后访问的资源统计, 可以咨询一下思科的 firepower
- ✓ 问题：架设环境需要的硬件设备需要哪些
- ✓ 回答：acs, asa, anyconnect 客户端
- ✓ 问题：U-Turn 能否在同一 ASA 上实现? 即客户端 VPN 拨号后, 所有流量都走 ASA, 并且通过这台 ASA 访问 Internet?
- ✓ 回答：可以在同一 asa 实现。比如：nat (outside, outside) xxx
- ✓ 问题：ASA 升级到 9.0 以上版本, 在做访问控制列表的时候, 对于 ipv4 流量, 必须写 ipv4 吗?? 发现 5510 设备用 9.1 的时候写访问控制列表只用协议 ip 的时候流量不通。
- ✓ 回答：不是必须写 any4。当 9.1 不通的时候, 可以考虑看下 nat 和 acl 的配置。并不仅仅是 acl 的配置。若有未解决的, 建议开 case 看一下
- ✓ 问题：思科是否有 IDP 类设备
- ✓ 回答：建议你咨询并了解一下 思科的 Firepower。可以联系思科销售
- ✓ 问题：我生产的 ASA5550 系列软件版本 8.2, 出现问题是：ASDM 可以登录, 但是配置菜单载入到 50%就停止了, 最终结果是我无法用 ASDM 来管理配置了, 请问如何解决,

是否可以重启。现在我只能通过命令行来处理了。

- ✓ 回答：检查一下 java 版本，查一下 asd 的 release note，java 和浏览器的兼容性。

- ✓ 问题：anyconnect 手机端 只需要 license 支持，配置上有特殊之处吗？
- ✓ 回答：license ok 后，asa 上没有特殊配置之处。
- ✓ 问题：webvpn 的页面定制，除了用 ASDM 之外，还有什么更方便的方法吗？
- ✓ 回答：并没有
- ✓ 问题：tunnel-group sslvpn webvpn-attributes group-alias sslvpn enable-----//这个命令是啥意思啊，为啥一定要配呢？
- ✓ 回答：根据不通的条件，比如部门，设定不通的 alias。在登录的时候选择正确的 alias 登录。

- ✓ 问题：ASA5520 IOS 9.17 现在是不是有漏洞了？我看前几天还是推荐使用版本呢
- ✓ 回答：具体是指的哪一个漏洞呢？

- ✓ 问题：cisco 公司内部 vpn 用的是什么协议？webssl or ?
- ✓ 回答：ssl
- ✓ 问题：是否有 mtu 需要考虑？大包可否分片？
- ✓ 回答：没有
- ✓ 问题：hello 包 timeout 是多少？在家连接时 VPN 老是断线可能是什么问题？(不连 vpn 线路很好)
- ✓ 回答：断线的原因是多样化的。建议开 TAC case 深入检查。