



数据无形 传输有度

工业以太网的网络安全

- 概况
- 交换安全
- 防火墙
- 虚拟局域网VPN
- 结论



**HIRSCHMANN**

A **BELDEN** BRAND

# 概況

## 信息安全

定义：

- “采用一系列的手段来防止未经认证（授权）的使用、恶意的使用、拒绝正常使用或篡改信息、数据或资源....”



## 安全威胁

- ❑ 在工厂网络环境中，互联的各种设备会越来越多
- ❑ 工厂网络环境会越来越的接受来自外部的影响
- ❑ 发动网络攻击的“武器（工具）”很容易得到
- ❑ 当前广泛使用的网络协议(TCP/IP)和网络技术(Ethernet)比较容易受攻击
- ❑ 网络攻击的源头很难追溯和确定

**Attacks represent a heightened risk for production environments**

## 网络攻击

- 网络攻击有不同的目的性：
  - 系统入侵(hacking)
  - 破坏 / 网络恐怖袭击
  - 信息偷窃
  - 网站攻击
  - 报仇、泄恨
  - 错误的、不经意的误操作

## 网络攻击的形式

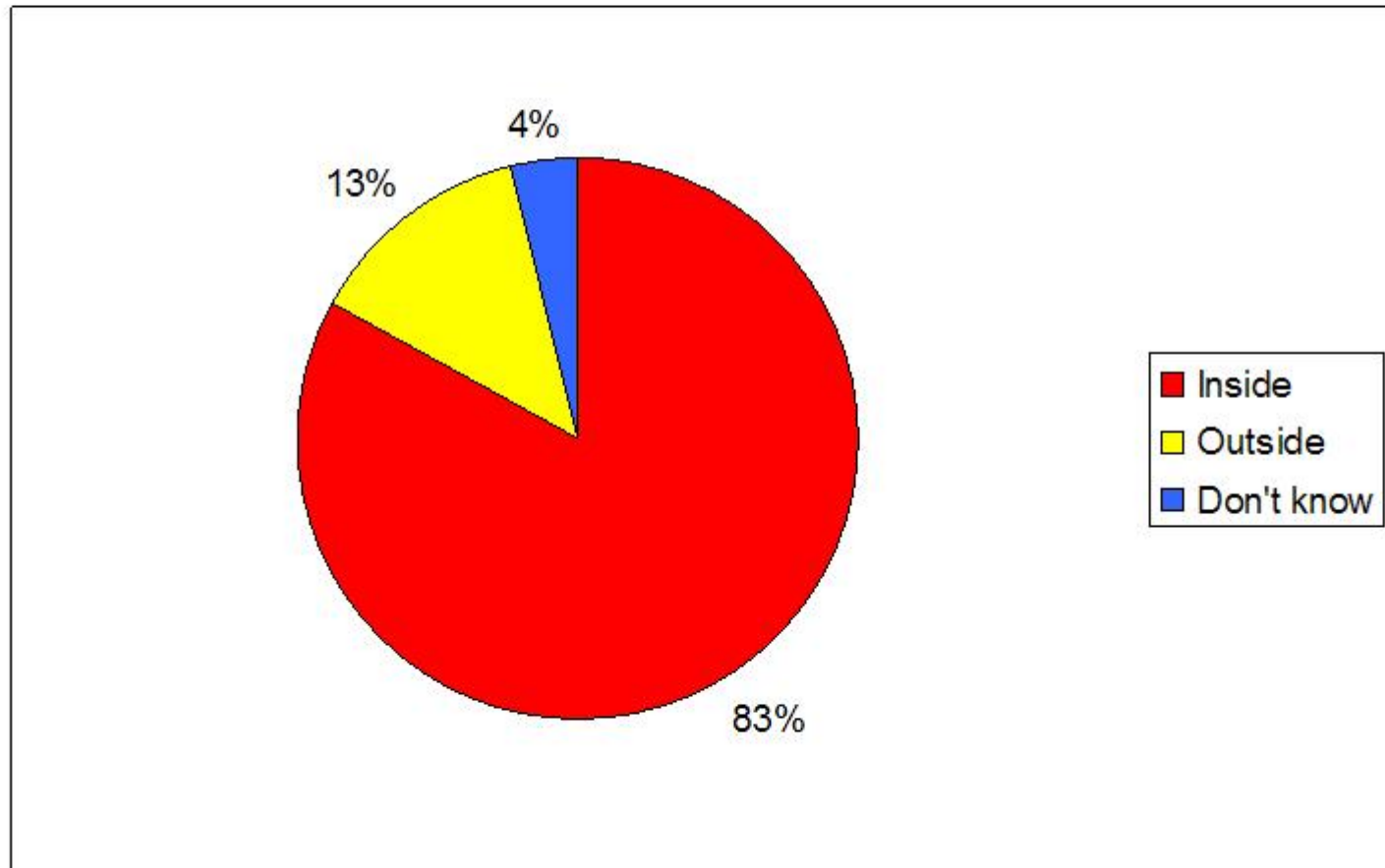
- ❑ 拒绝服务攻击(DOS)
  - ✓ 病毒 / 特洛伊木马 / 蠕虫
  - ✓ 耗费系统资源 (TCP SYN, ICMP, ...)
  - ✓ 利用系统弱点, TCP/IP
- ❑ 访问攻击
  - ✓ 密码破解
  - ✓ 假冒, 欺骗
- ❑ 信息收集 / 探测
  - ✓ 截获, 窃听
  - ✓ 探测TCP, ICMP

## 为什么要保护网络？

- 网络是整个公司的核心
  - 网络承载了越来越多的敏感数据：
    - 各种文件、文档
    - 市场研究报告
    - 库存管理
    - 客户信息
    - 商业和竞争对手信息
    - .....
- 如果网络失效会发生什么 ??



您认为网络安全攻击来自公司内部或外部的比重各是多少？





Nessus  
Vulnerability Scanner

Nessus is brought to you by:

**TENABLE**  
Network Security

[ABOUT](#)

[FEATURES](#)

[PLUGINS](#)

[DOCUMENTATION](#)

[COMPLIANCE](#)

[NEWS](#)

[DEMO](#)

[DOWNLOAD](#)

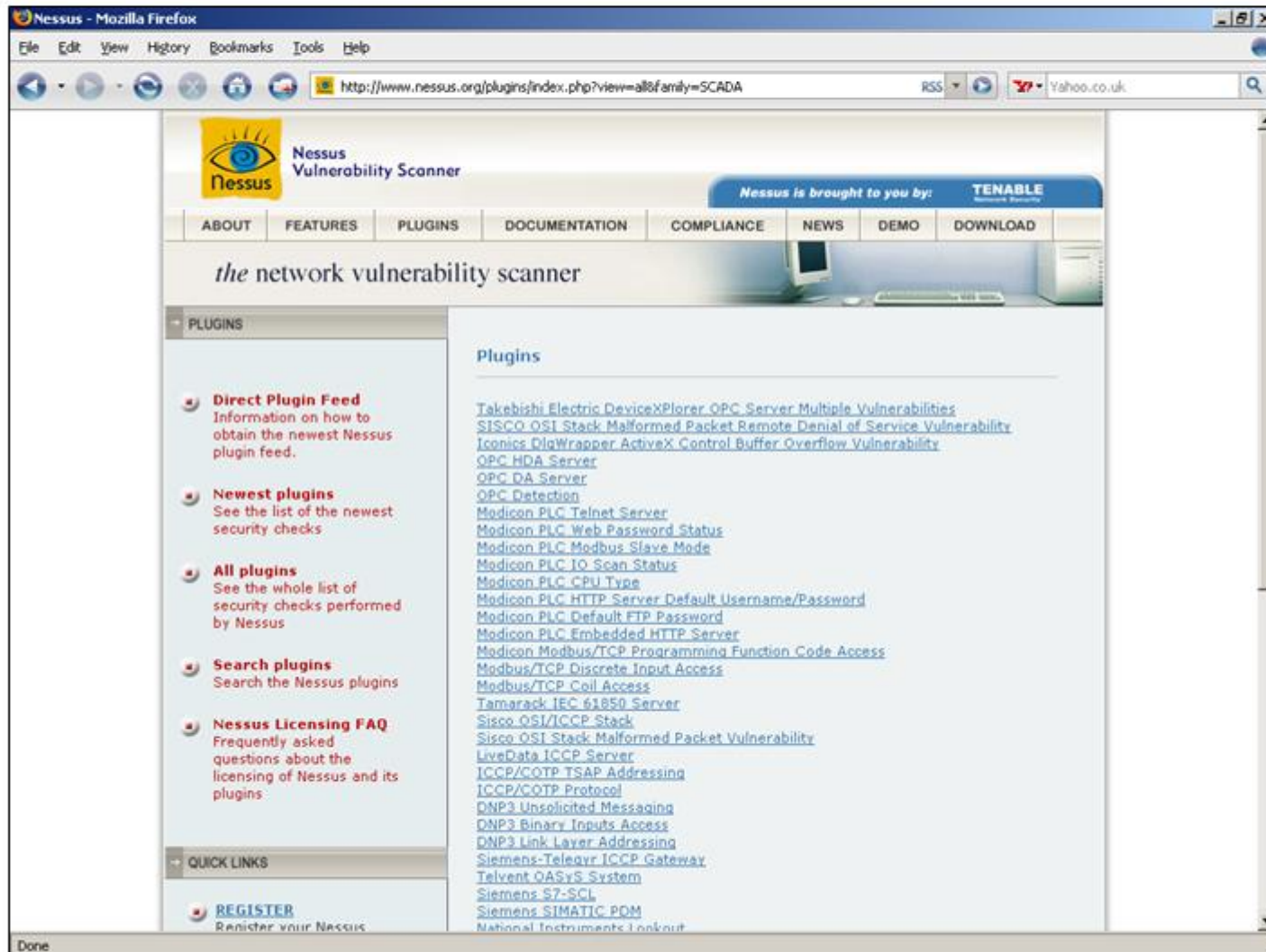
The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.

*the network  
vulnerability scanner...*

[→ LATEST NEWS](#)

[→ QUICK LINKS](#)

- Nessus是全球最流行的网络脆弱性（易受攻击性）扫描软件
- 全球有超过75,000个公司或组织在使用它



Nessus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nessus.org/plugins/index.php?view=all&family=SCADA

Nessus Vulnerability Scanner

Nessus is brought to you by: **TENABLE**

ABOUT FEATURES PLUGINS DOCUMENTATION COMPLIANCE NEWS DEMO DOWNLOAD

the network vulnerability scanner

PLUGINS

- Direct Plugin Feed**  
Information on how to obtain the newest Nessus plugin feed.
- Newest plugins**  
See the list of the newest security checks
- All plugins**  
See the whole list of security checks performed by Nessus
- Search plugins**  
Search the Nessus plugins
- Nessus Licensing FAQ**  
Frequently asked questions about the licensing of Nessus and its plugins

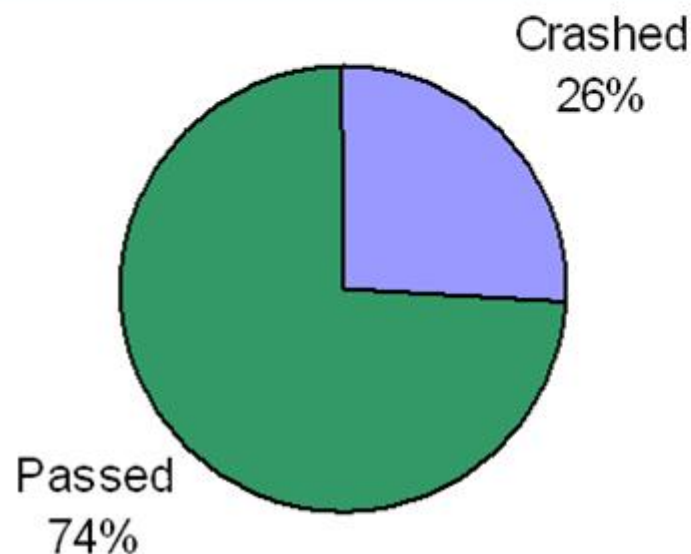
QUICK LINKS

- REGISTER**  
Register your Nessus

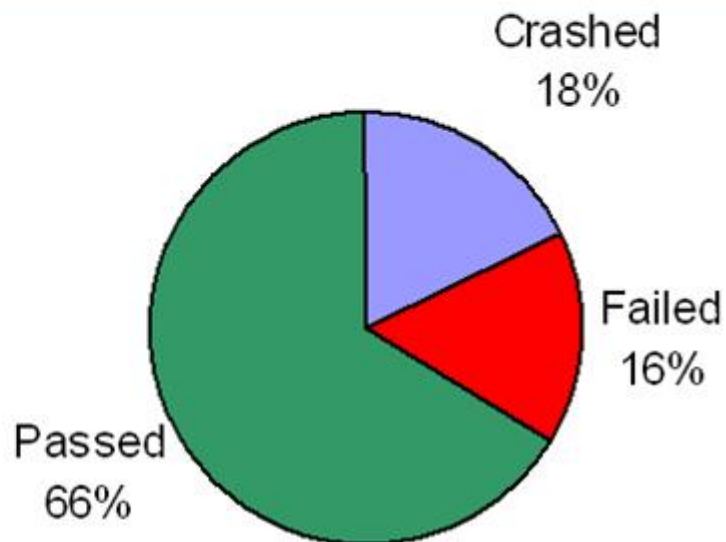
Plugins

- [Takebishi Electric DeviceXplorer OPC Server Multiple Vulnerabilities](#)
- [SISCO OSI Stack Malformed Packet Remote Denial of Service Vulnerability](#)
- [Iconics DlgWrapper ActiveX Control Buffer Overflow Vulnerability](#)
- [OPC HDA Server](#)
- [OPC DA Server](#)
- [OPC Detection](#)
- [Modicon PLC Telnet Server](#)
- [Modicon PLC Web Password Status](#)
- [Modicon PLC Modbus Slave Mode](#)
- [Modicon PLC IO Scan Status](#)
- [Modicon PLC CPU Type](#)
- [Modicon PLC HTTP Server Default Username/Password](#)
- [Modicon PLC Default FTP Password](#)
- [Modicon PLC Embedded HTTP Server](#)
- [Modicon Modbus/TCP Programming Function Code Access](#)
- [Modbus/TCP Discrete Input Access](#)
- [Modbus/TCP Coil Access](#)
- [Tamarack IEC 61850 Server](#)
- [Sisco OSI/ICCP Stack](#)
- [Sisco OSI Stack Malformed Packet Vulnerability](#)
- [LiveData ICCP Server](#)
- [ICCP/COTP TSAP Addressing](#)
- [ICCP/COTP Protocol](#)
- [DNP3 Unsolicited Messaging](#)
- [DNP3 Binary Inputs Access](#)
- [DNP3 Link Layer Addressing](#)
- [Siemens-Televar ICCP Gateway](#)
- [Telvent OASys System](#)
- [Siemens S7-SCI](#)
- [Siemens SIMATIC PDM](#)
- [National Instruments Linkout](#)

Done



Netwox – 拒绝服务攻击



Nessus – 弱点攻击

*Results of 51 different TOCSSiC\* tests on networked industrial control devices - mainly PLCs - using Netwox and Nessus*



**HIRSCHMANN**

A **BELDEN** BRAND

# 交换安全



Automation and Network Solutions

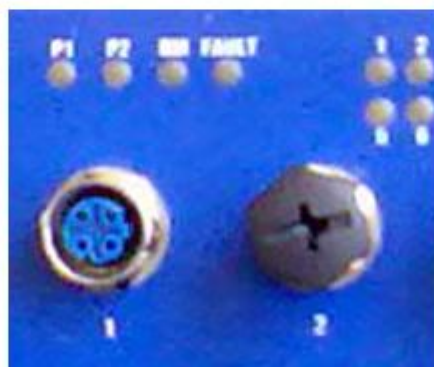
**The most dangerous hackers work in your own company.**

**Industrial Networking**

**Security Router  
EAGLE**

Do you really know who in your company has access to your production results? Accidents in production can happen and not just when people working at night press the wrong button or download malicious software. Protect yourself against such attacks to your company network: with the Hirschmann EAGLE, the first industrial security router/firewall supporting virtual private networking and firewall functions. It prevents unwanted "intrusions" ensuring that not only your network but also your production process stays secure and productive. The EAGLE Security Router provides the safety and reliability you've come to expect from Hirschmann. [www.hirschmann.com](http://www.hirschmann.com)

Hirschmann. Solutions for Communication.



## 未使用的端口

- 关闭未使用的端口
- 无法使用网络

149.218.17.105 Railswitch - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://

**System** HIRSCHMANN

System

Devicestatus

Alarmstarttime -

Alarmreason -

System data

Name: Hirschmann RS 2

Location: Hirschmann Railswitch

Contact: nann Automation and Control GmbH

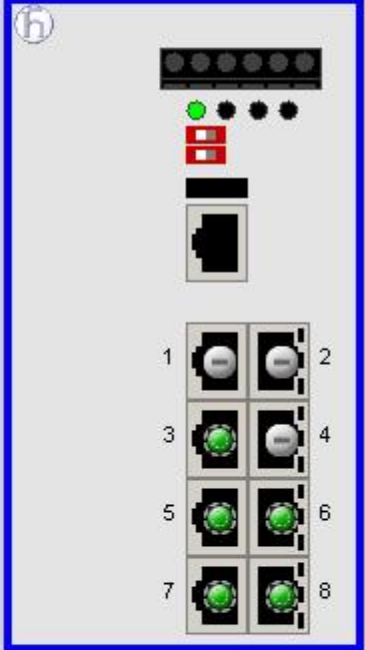
Basic module: RS20-0800T1T1 SDAPHH HW:1.30

Power supply 1/2: present / present

Temperature (°C): 0 33 70

Uptime: 5 day(s), 1:27:36

Device view



1 2

3 4

5 6

7 8

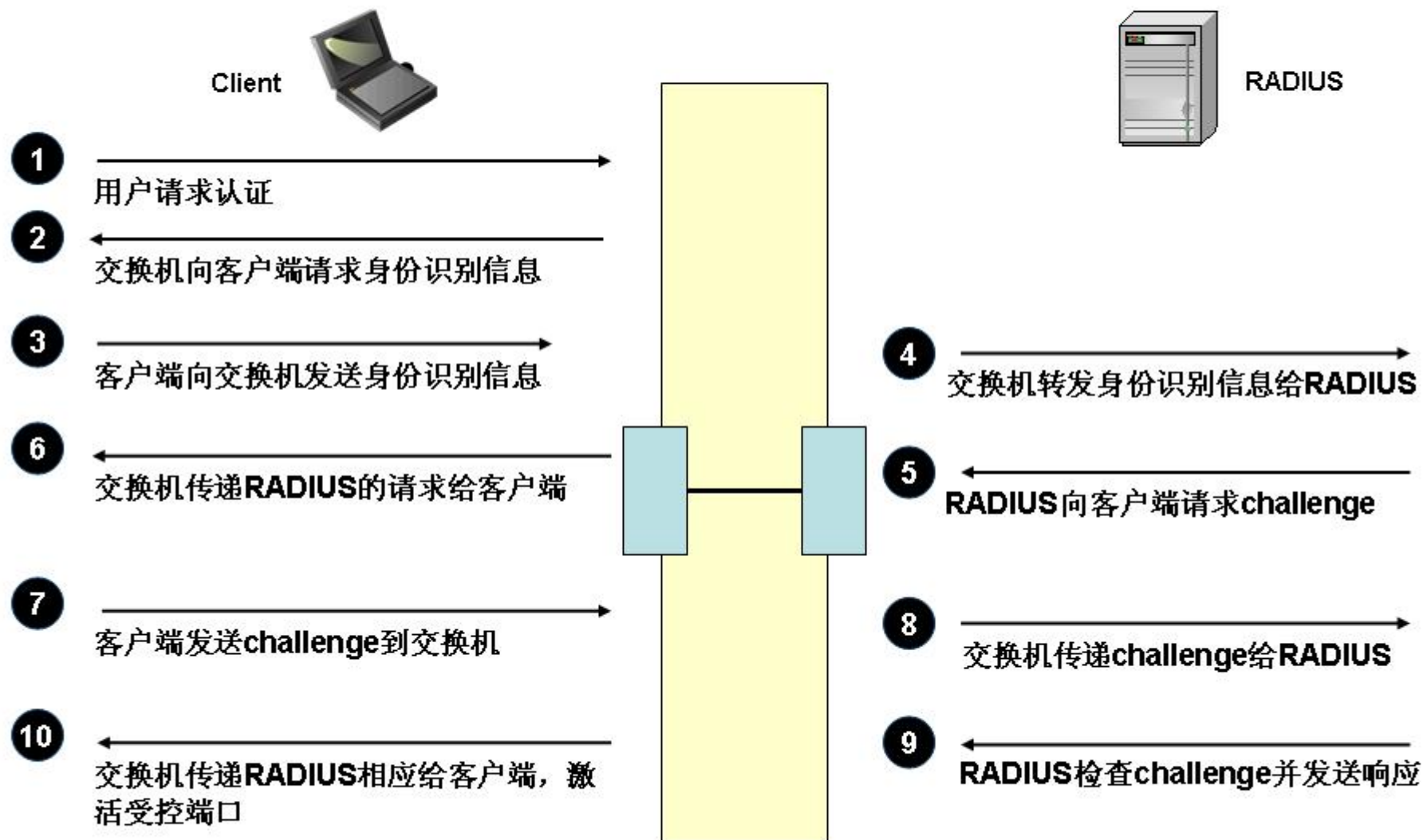
Set Reload Help

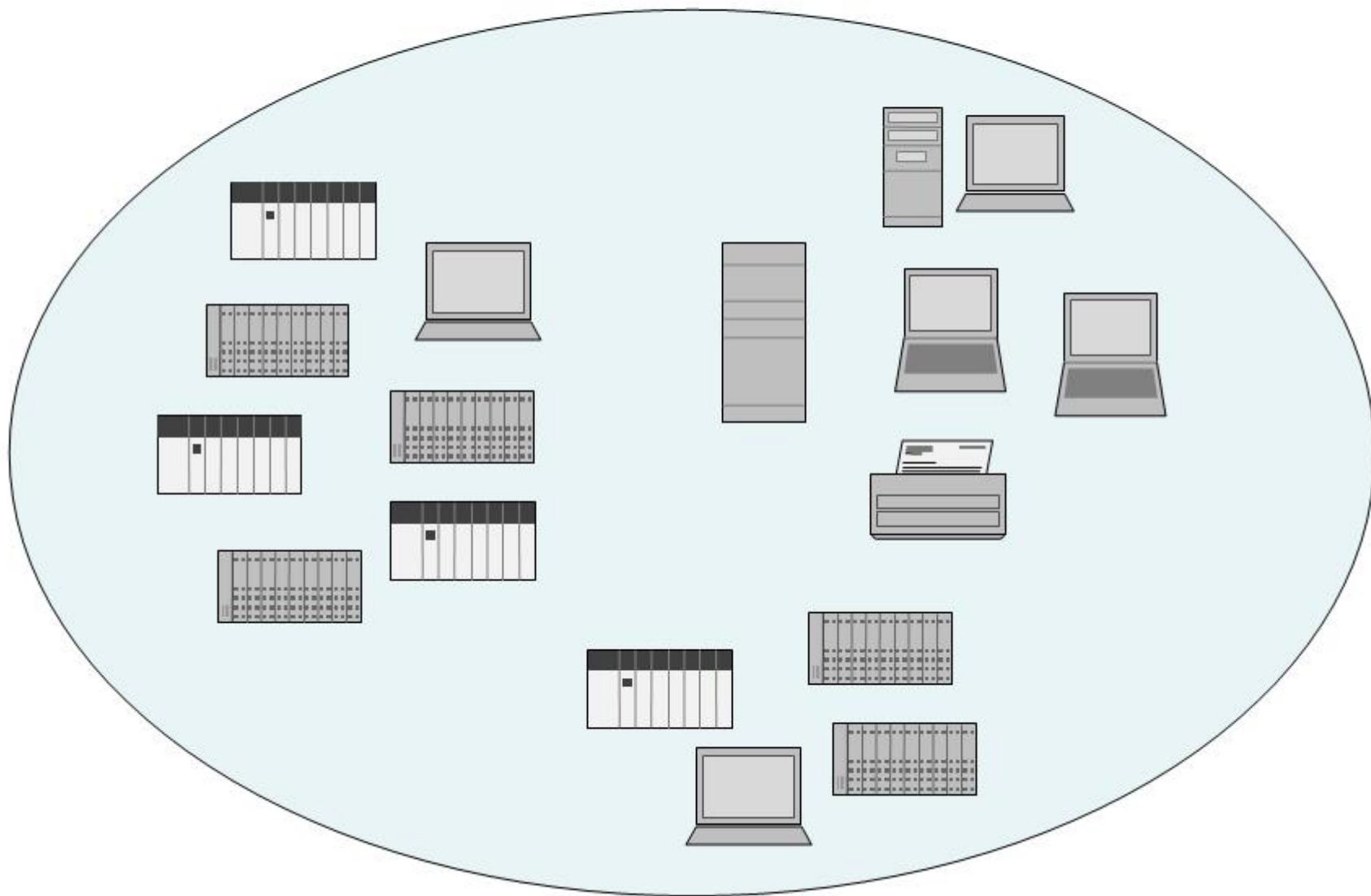
Applet com.hirschmann.deviceMgmt.quickstart.Start started

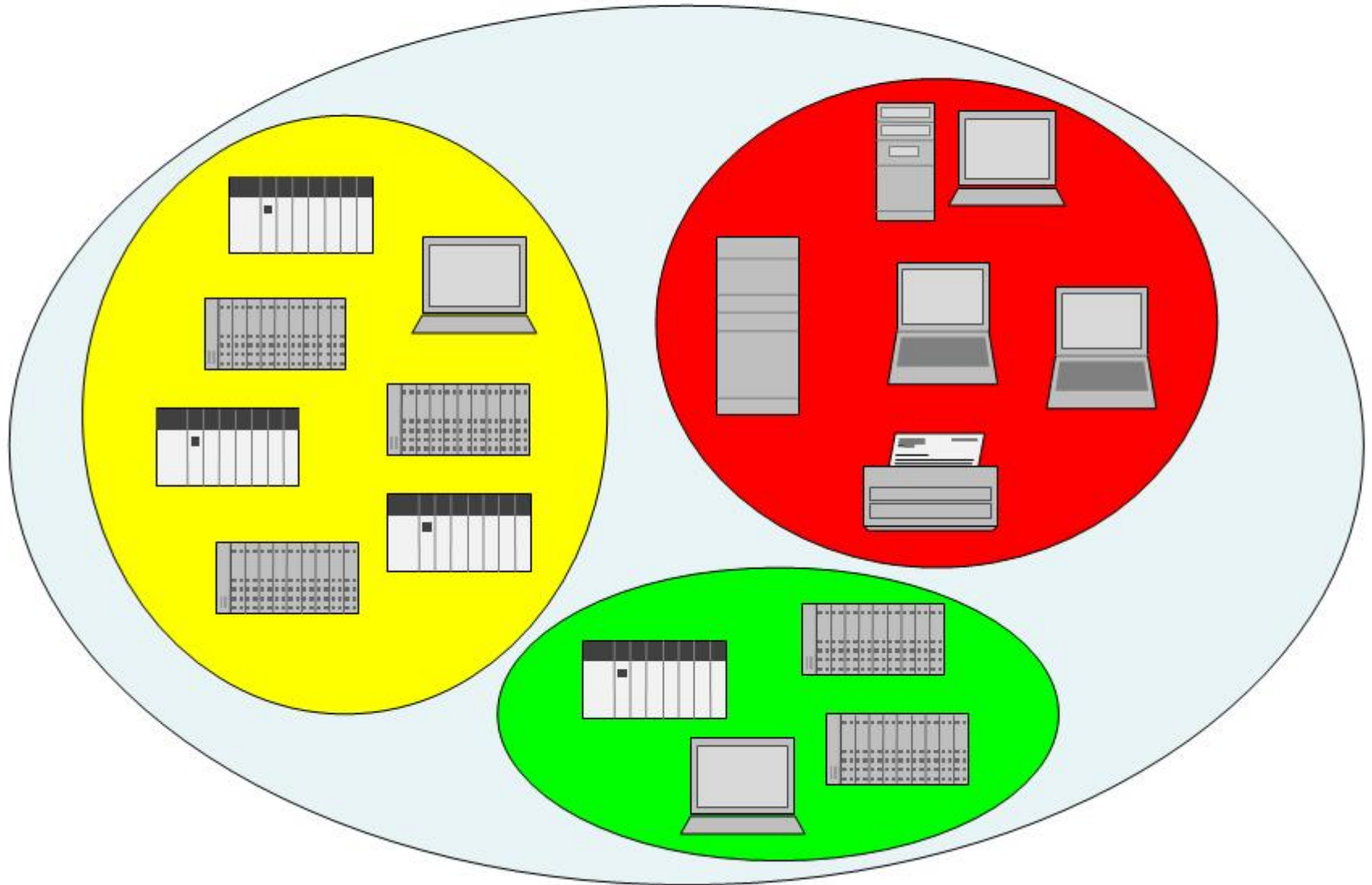


- 只有指定的设备才能够访问网络
  - MAC address
  - IP address
  
- 否则...
  - 发送消息给管理站点报告非法访问
  - 自动关闭端口

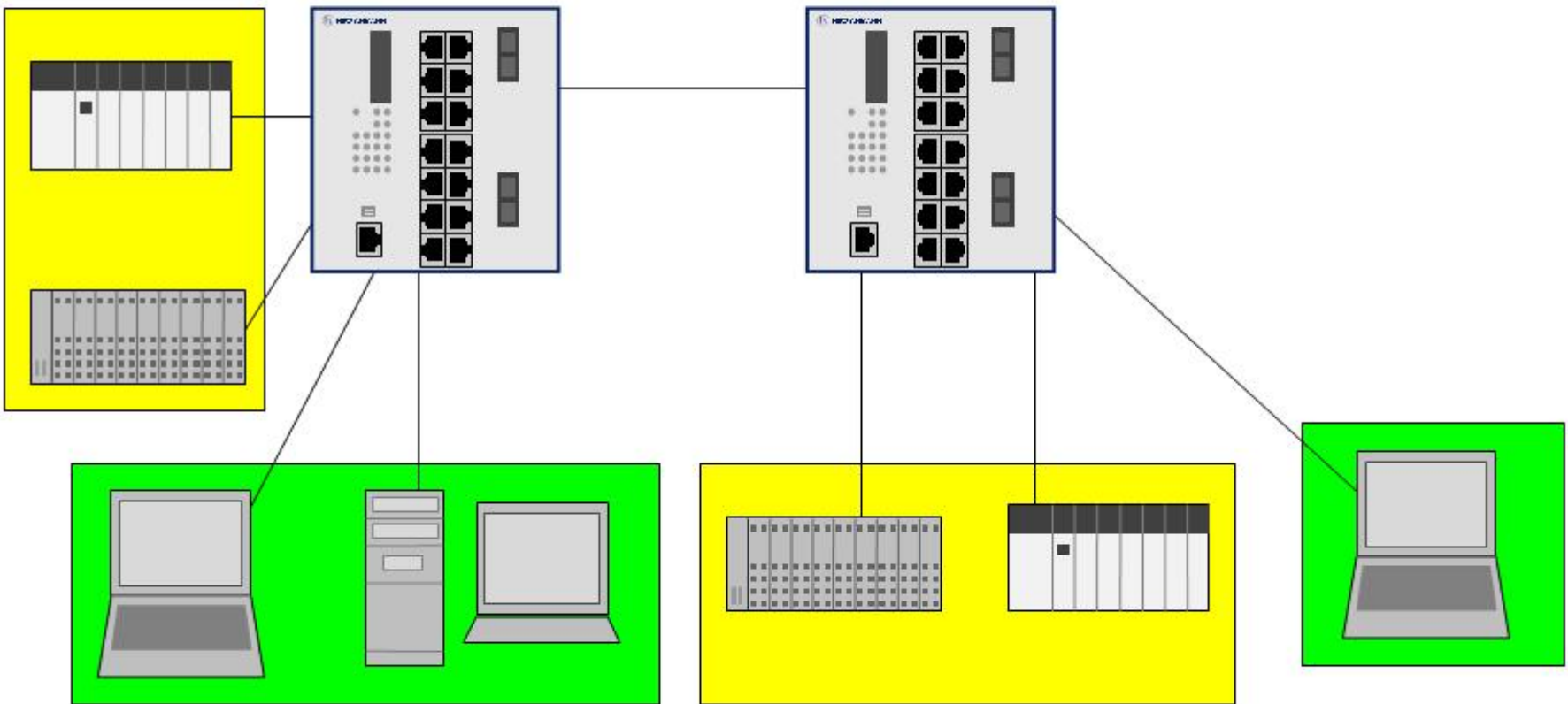
Module	Port	Port Status	Allowed MAC Address	Current MAC Address	Allowed IP address	Action
1	1	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	2	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	3	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	4	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	5	enabled	00:00:00:00:00:00	08:00:20:0A:34:7E	0.0.0.0	none
1	6	enabled	00:00:00:00:00:00	00:80:63:39:F8:85	0.0.0.0	none
1	7	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	8	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none

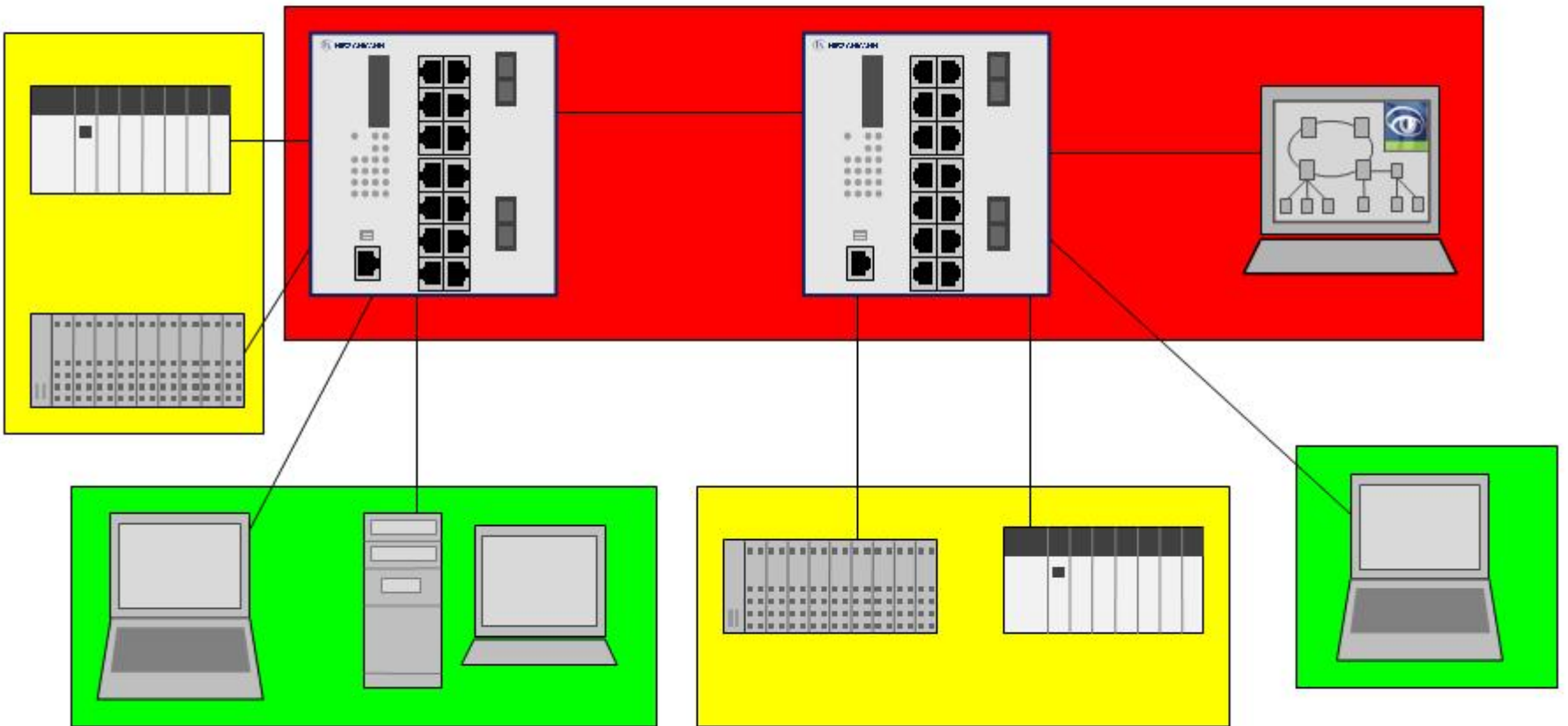






# 每台交换机承载多个VLAN





- SNMPv1
- SNMPv2
- SNMPv3
- Telnet
- SSH
- Web Interface



## Acronyms:

SNMP – 简单网络管理协议

SSH – 安全壳



**HIRSCHMANN**

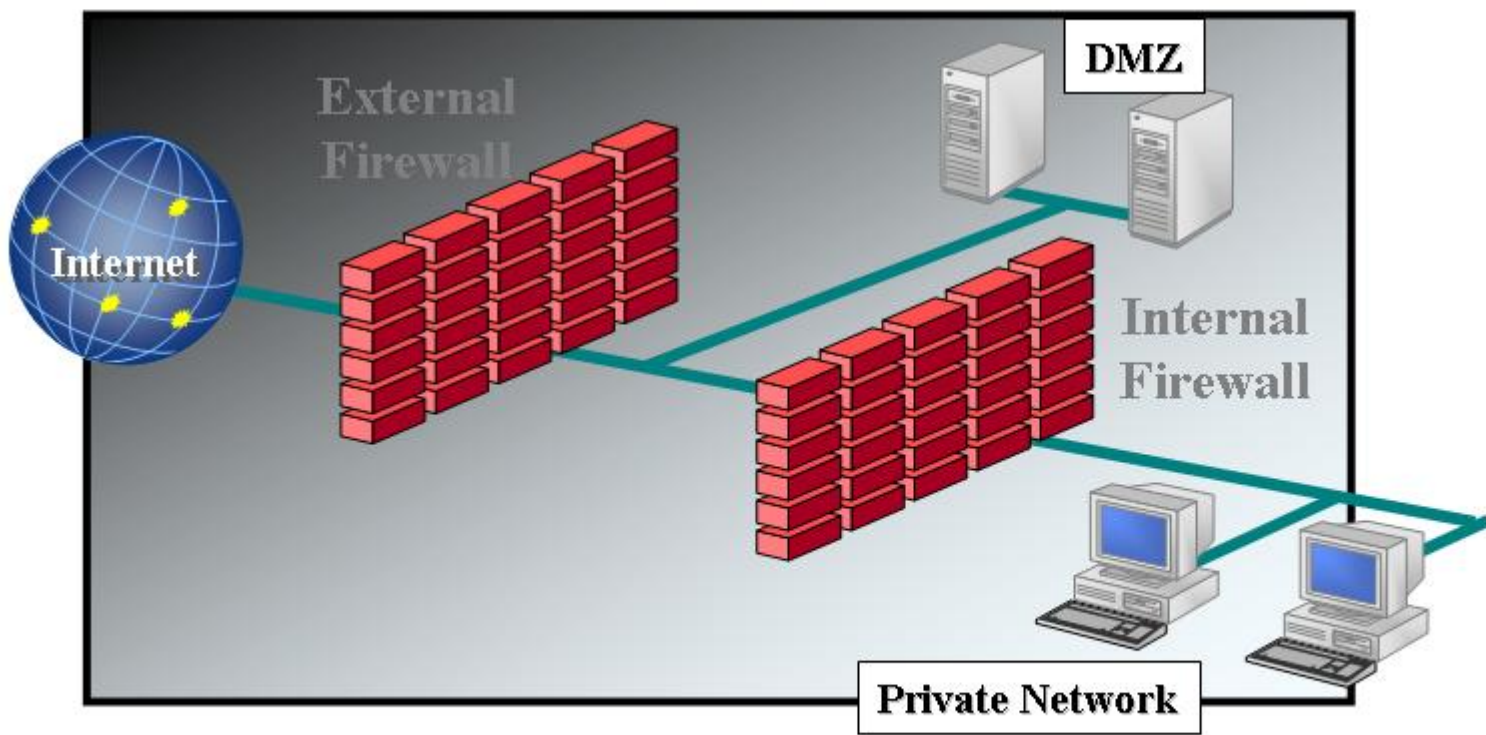
A **BELDEN** BRAND

# 防火墙



# 什么是防火墙?

- 防火墙是一个或一组系统，用于在两个网络之间执行访问控制策略



- 基本功能
  - 保护来自非安全网络的攻击
  - 隐藏内部网络架构
- 高级功能
  - 访问控制: 在何时以及多少台终端可以互相访问
  - 用户控制: 什么用户可以访问什么服务
  - 协议和服务控制: 什么协议和服务可以在什么端口运行
  - 数据控制: 什么样的数据可以被发送和接收
  - 记录, 记账, 审核
  - 在攻击或失效发生时报警
  - 防病毒支持

- 防火墙在以下情况下只能提供有限的保护甚至是无法提供保护:
  - 内部攻击
  - 基于许可连接的攻击
  - 恶意软件攻击如特洛伊(Trojans), 病毒, 间谍软件, 网络欺诈软件, 或具有破坏性的小程序 (ActiveX, Java Applets, JavaScript)
  - 被动式的攻击 (LAN刺探, 流量分析, etc.)
  - 移动计算机的不恰当使用
  - 可移动的媒介(USB...)



- 项目总的开销并不仅仅是初期的采购花费，还包括：
  - 设计费用(无论是内部的还是外部)
  - 日后的购买开销(硬件, 软件, 软件使用许可证等等其它选项的开支)
  - 安装、部署开销 (安装, 配置, 成档, 测试)
  - 培训
  - 管理
  - 维护

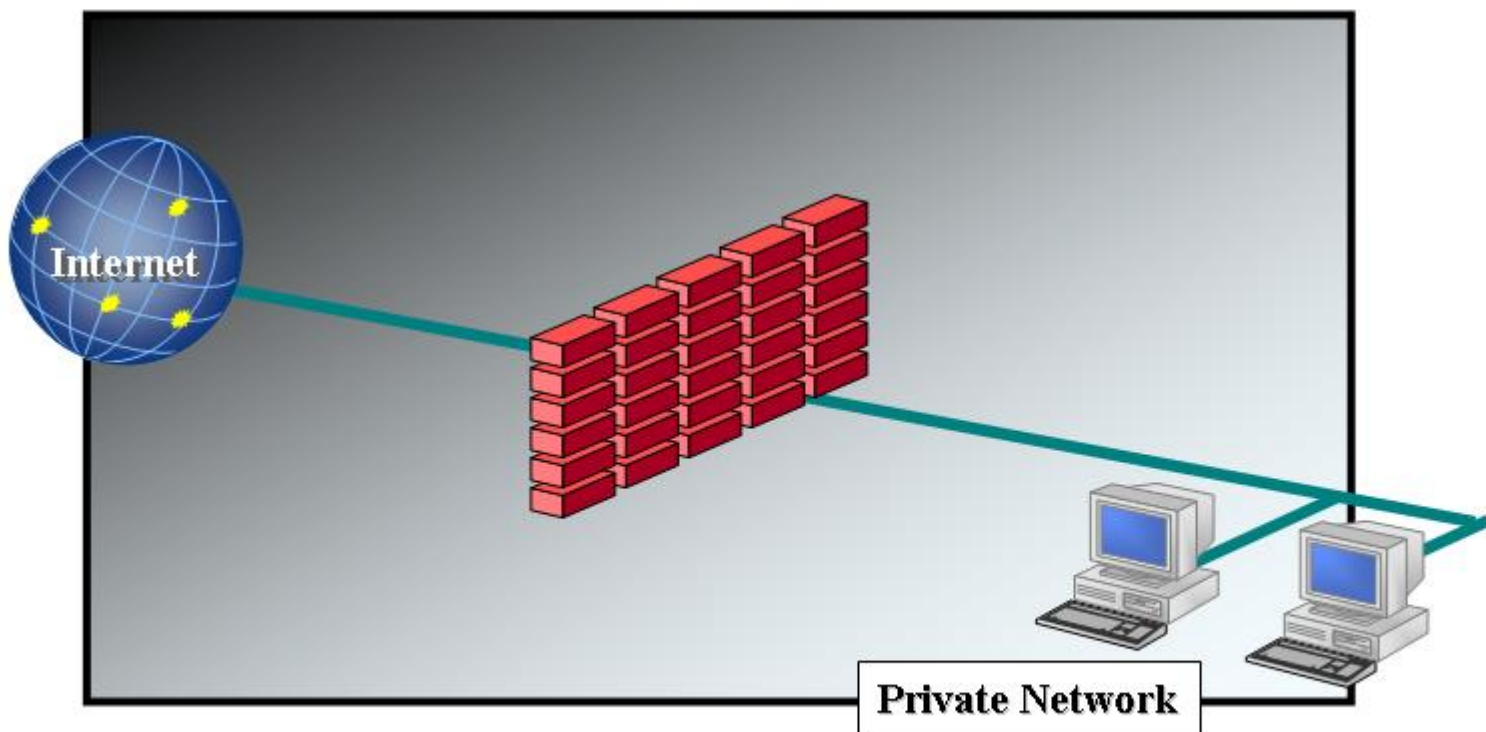


## 入侵测试

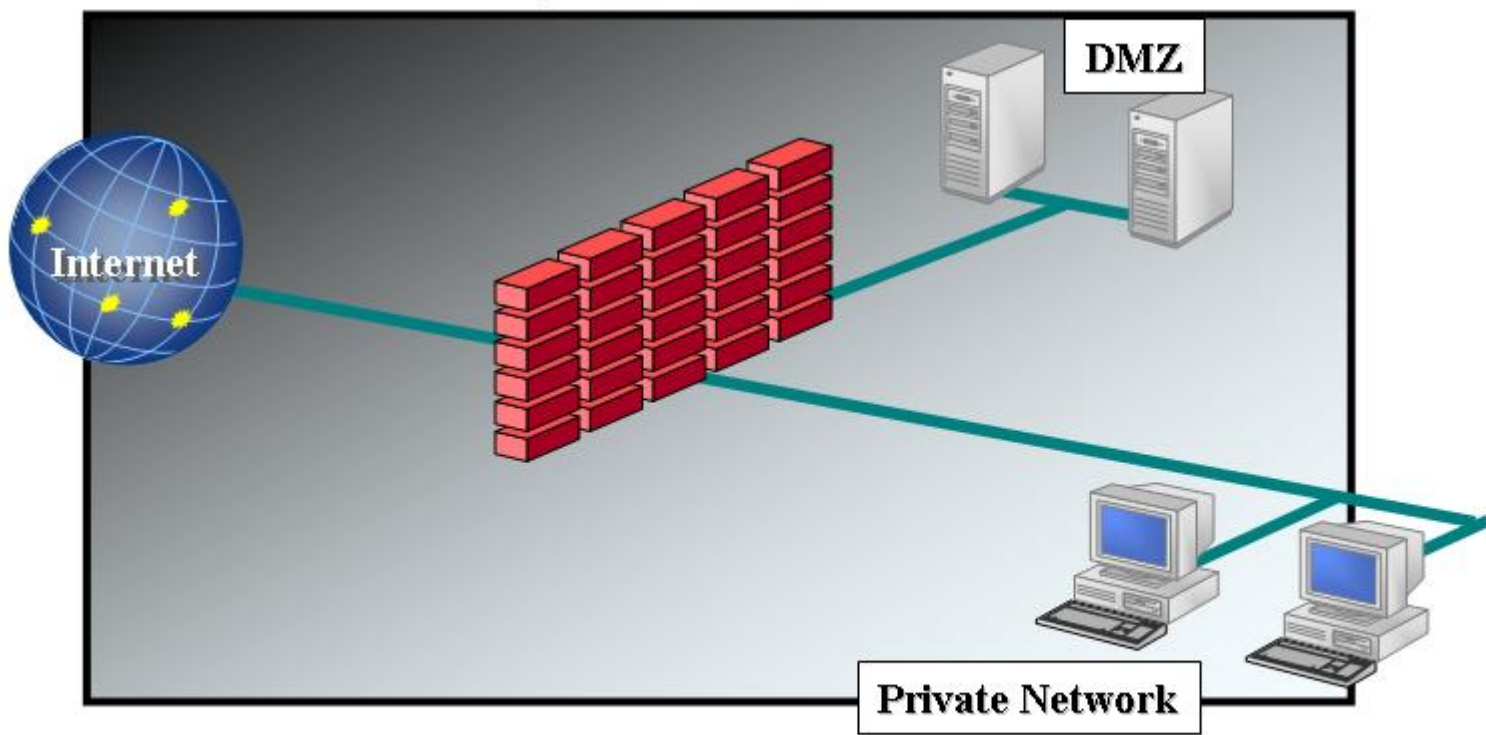
- 从外部发现网络安全漏洞
- 通过使用标准的或定制的攻击对网络安全进行测试，即模拟攻击
- 在有提前通知和没有提前通知的情况下测试网络安全
- 总结并做详细的技术报告
- 得出最终结论



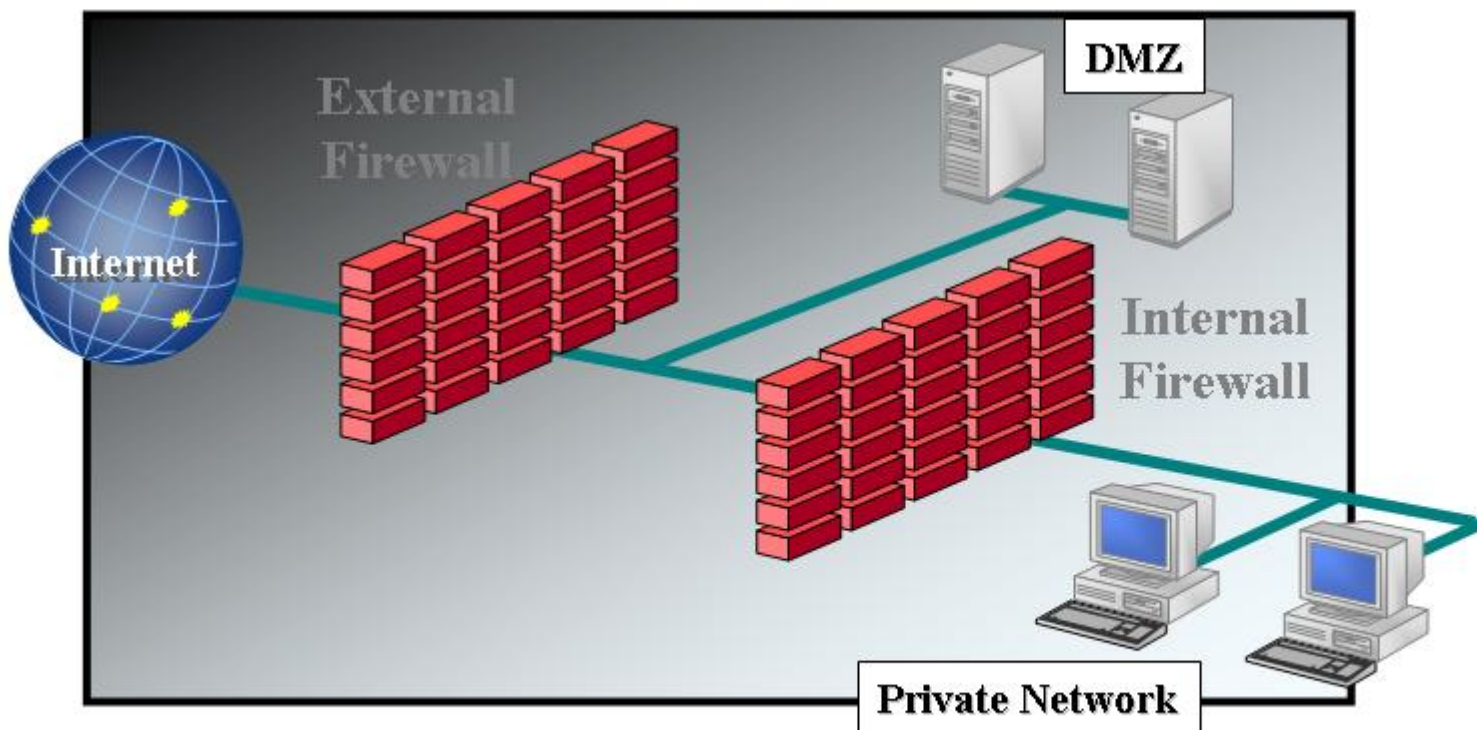
- 防火墙带有2个以太网接口
  - 一个用于连接安全网络
  - 另一个用于连接非安全网络



- 防火墙带有3个或更多接口
  - 一个用于连接安全网络
  - 另一个用于连接非安全网络
  - 还有一个可连接非武装区域

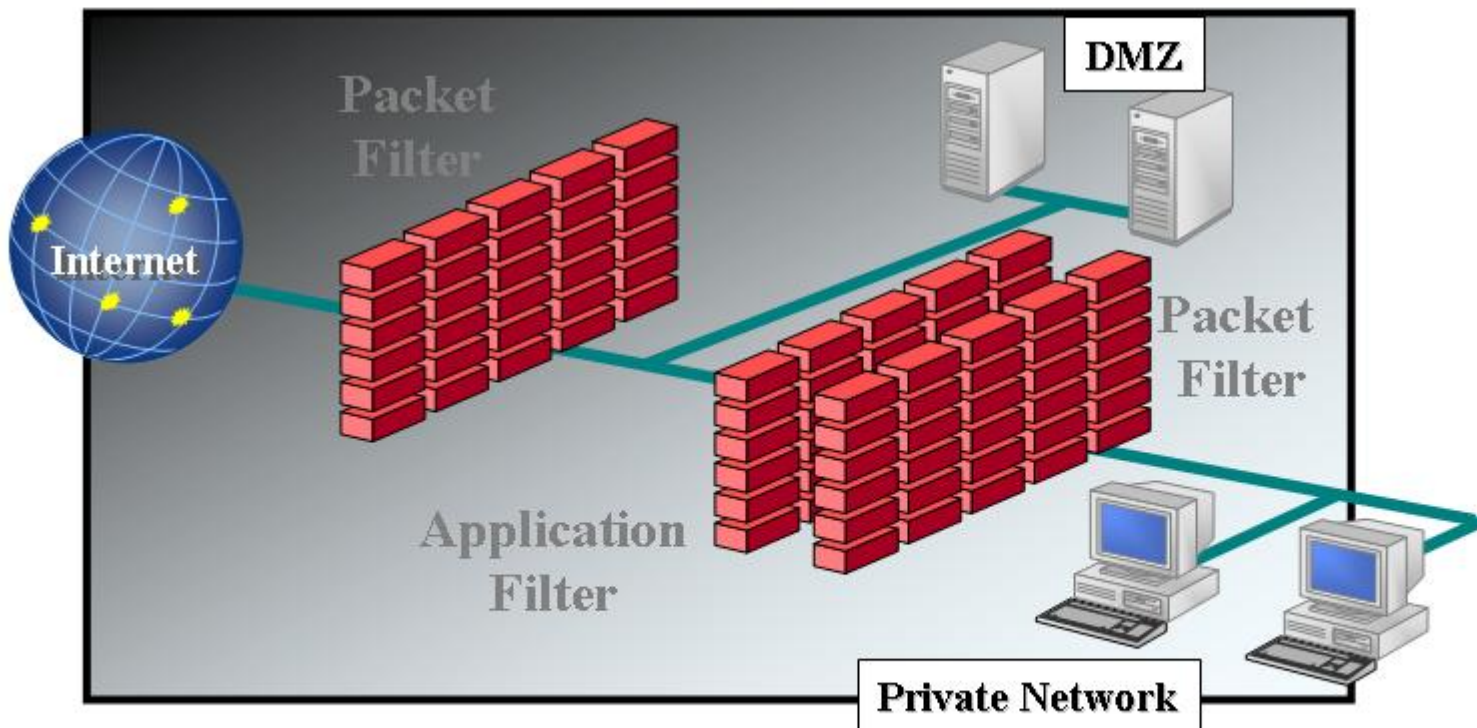


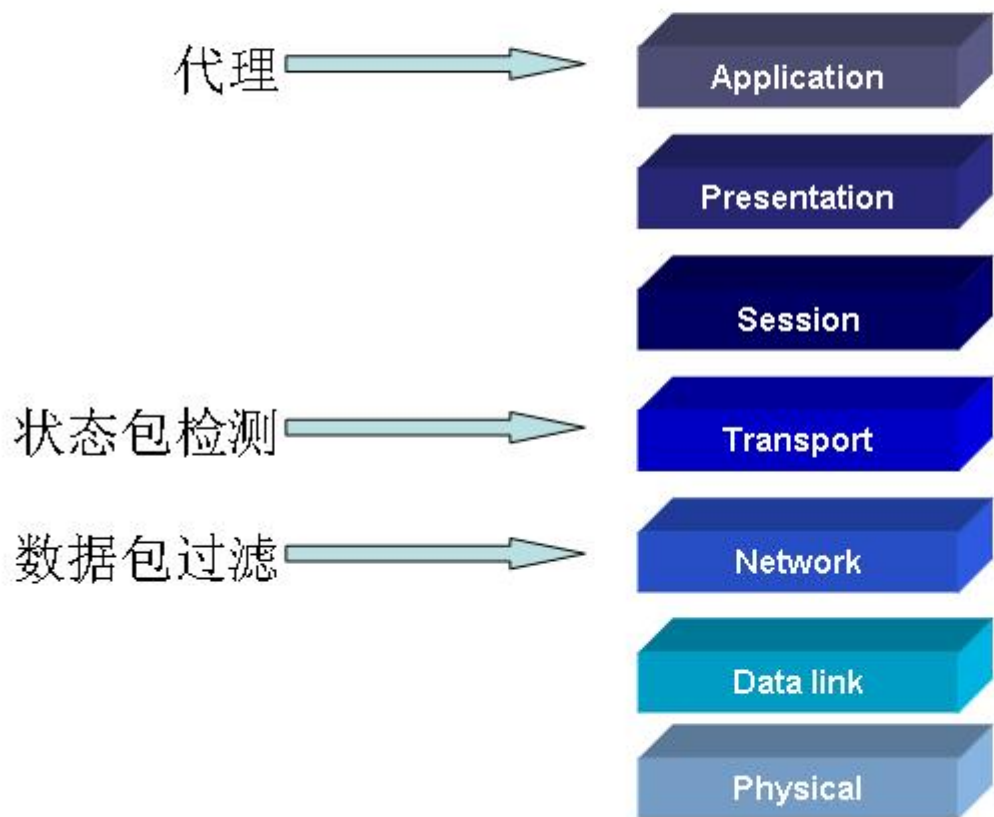
- 部署两个防火墙，两个防火墙的各一边连接DMZ



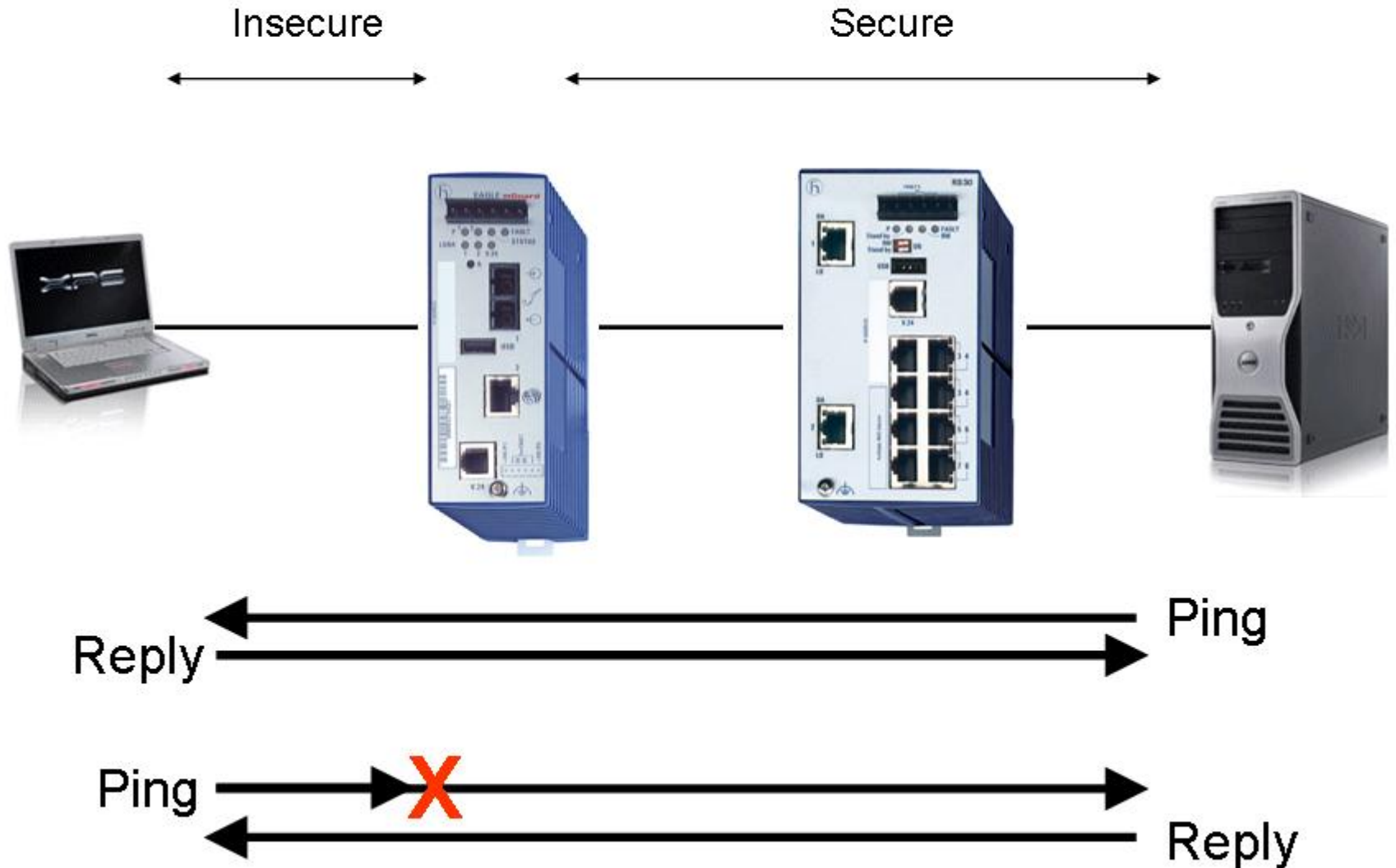


- 部署三个防火墙
- 分别用于不同的用途





- 在第 4 层分析数据通信 (传输层)
- 防火墙维护着一张设备通信表
- 只有当安全网络端发出通信请求时，来自非安全端的数据才被允许通过防火墙
  
- 优点
  - 检查连接状态
  - 比起应用层防火墙来说实现起来更便宜、更迅速
  
- 缺点
  - 不检查数据包内部的数据

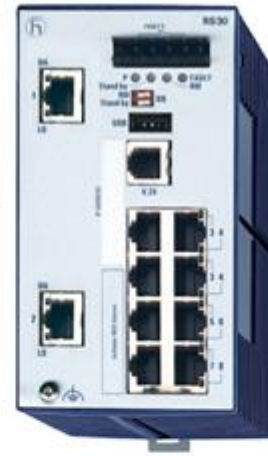


- 数据包在第3层 (网络层)被分析和检测.
  - 基于源IP地址
  - 基于源端口
  - 基于目的IP地址
  - 基于目的端口
  - 协议
- 访问规则定义了允许或拒绝什么样的通讯.
- 两个过滤逻辑:
  - “Deny all” (意味着所有没有显示说明允许的流量都将被拒绝)
  - “Laissez faire” (意味着所有没有显示说明拒绝的流量都将被允许)

- 特别注意
  - 只检查数据包的包头部分 – 而不是真正的数据本身 (payload有效负载)
  - 该功能在路由器中被经常引用 (访问控制列表)
- 优点
  - 速度快
- 缺点
  - 既不检查连接，也不检查“有效负载”本身
  - 可能需要定义许多的访问控制规则
  - 比较容易犯人为错误
  - 当网络结构发生该表示需要重新定义

Insecure

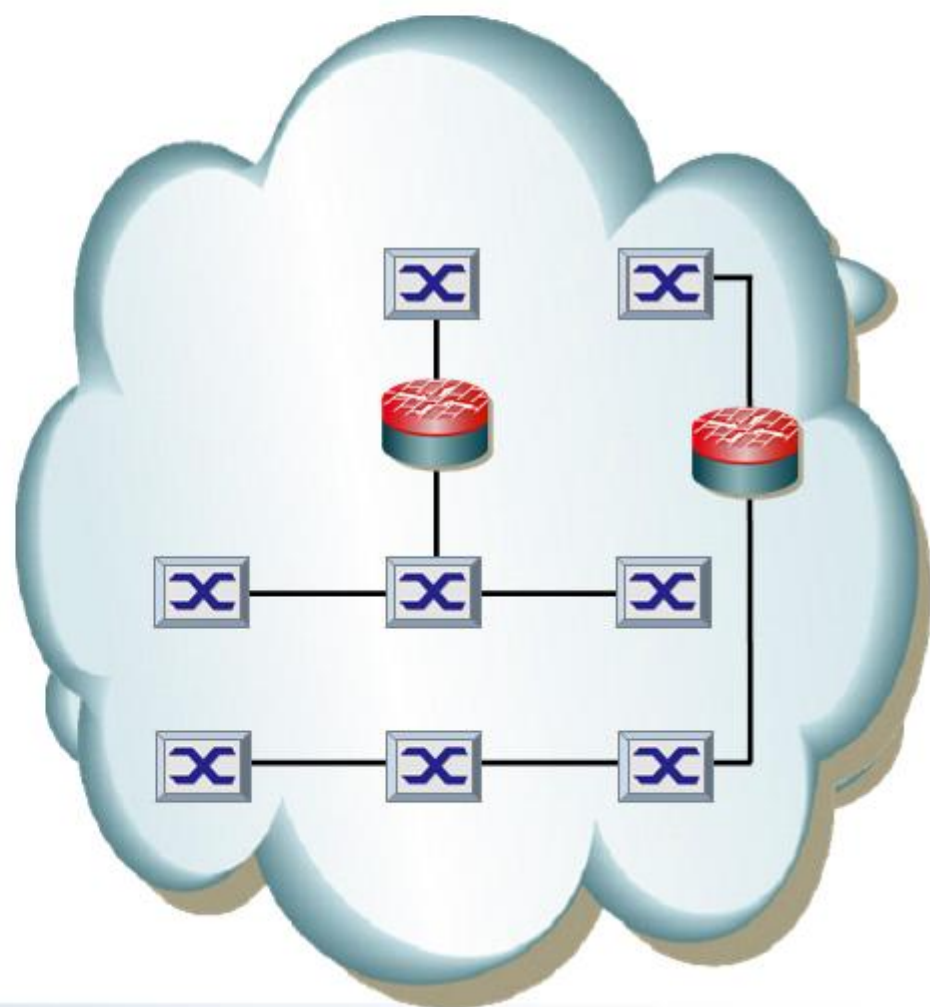
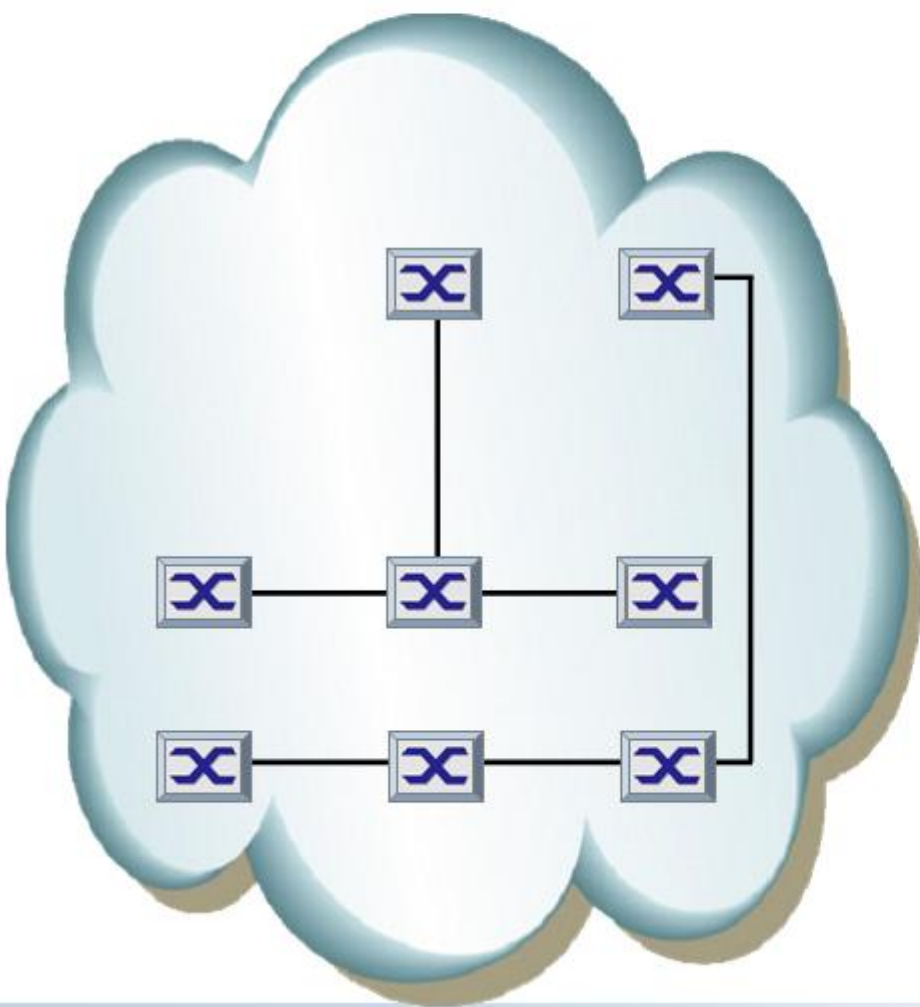
Secure



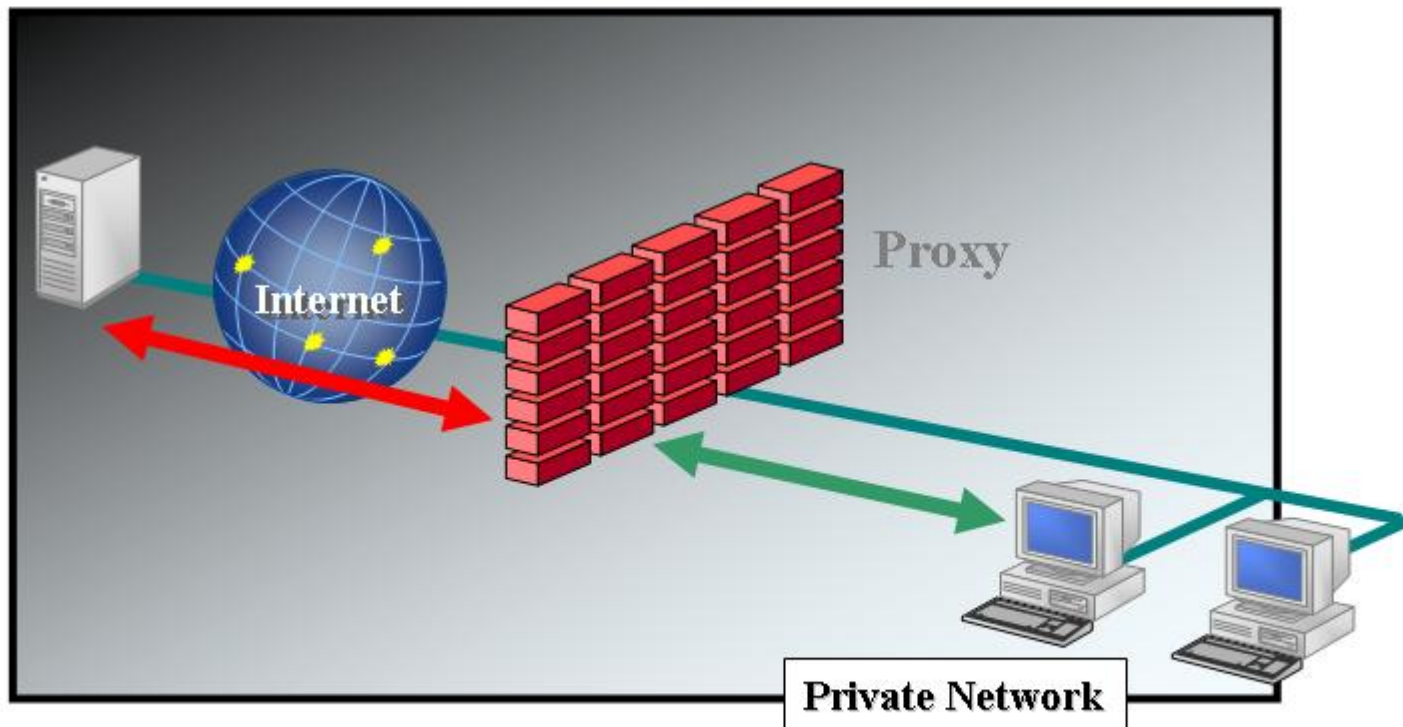
- 作为一个完整的网络，您在设计的时候需要考虑网络安全性
- 如果您准备给您现有的网络增加安全性呢？
- 在多数情况下，路由器即是防火墙。







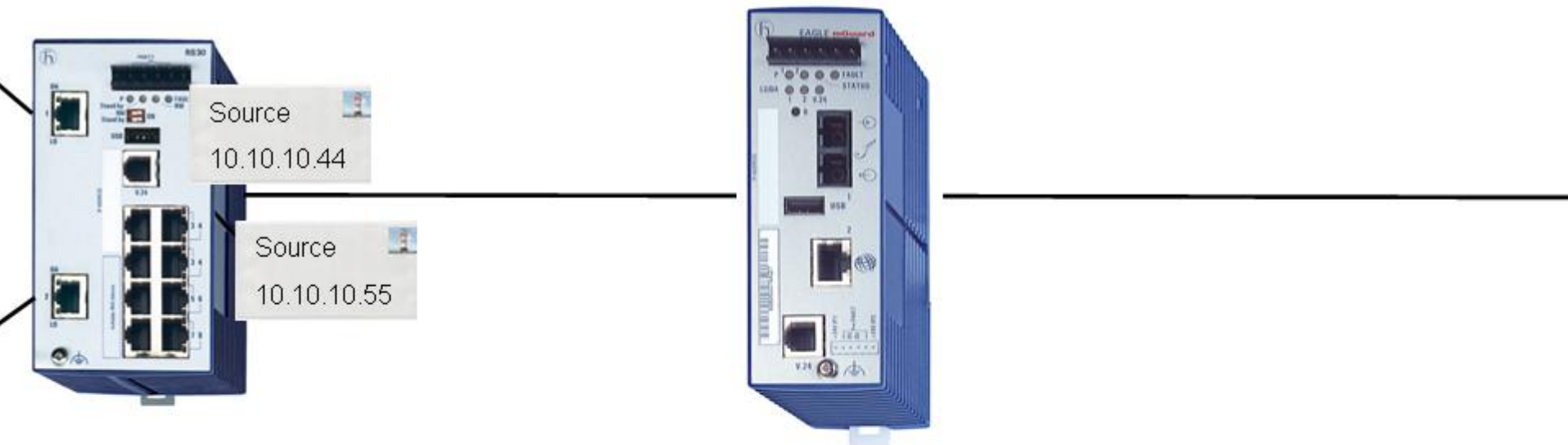
- 安全网络内的客户端和非安全网络内的服务器之间没有直接通信



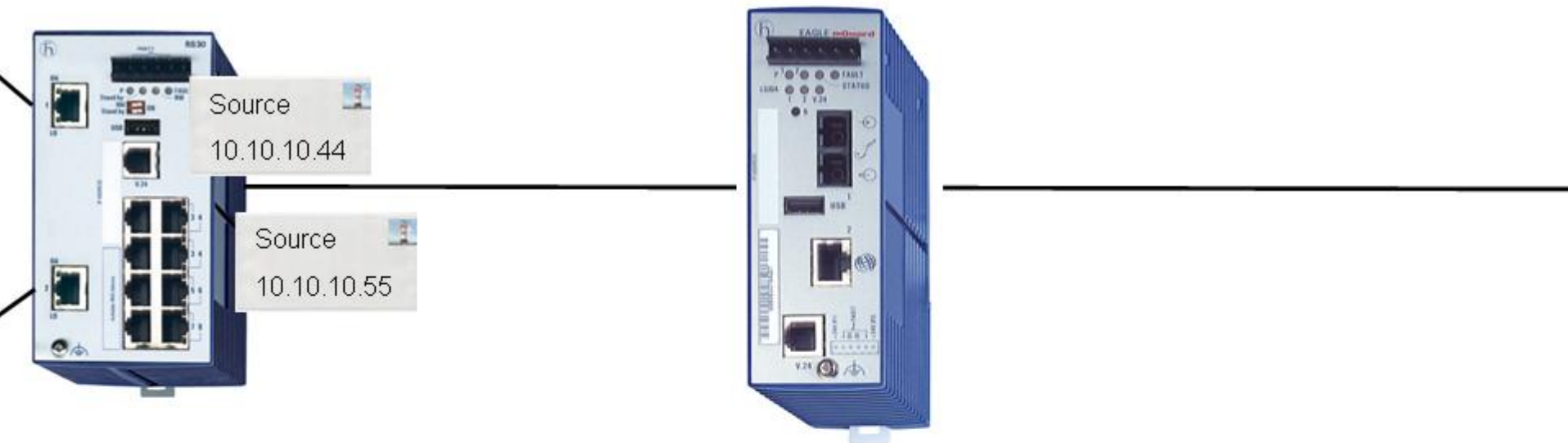
- 优点
  - 检查数据包中的有效载荷
  - 很高的安全性
- 缺点
  - 速度较状态包检测防火墙要慢
  - 价格更贵
- 事实是
  - 你希望的安全性越高，网络的性能就越差 (反之亦然)

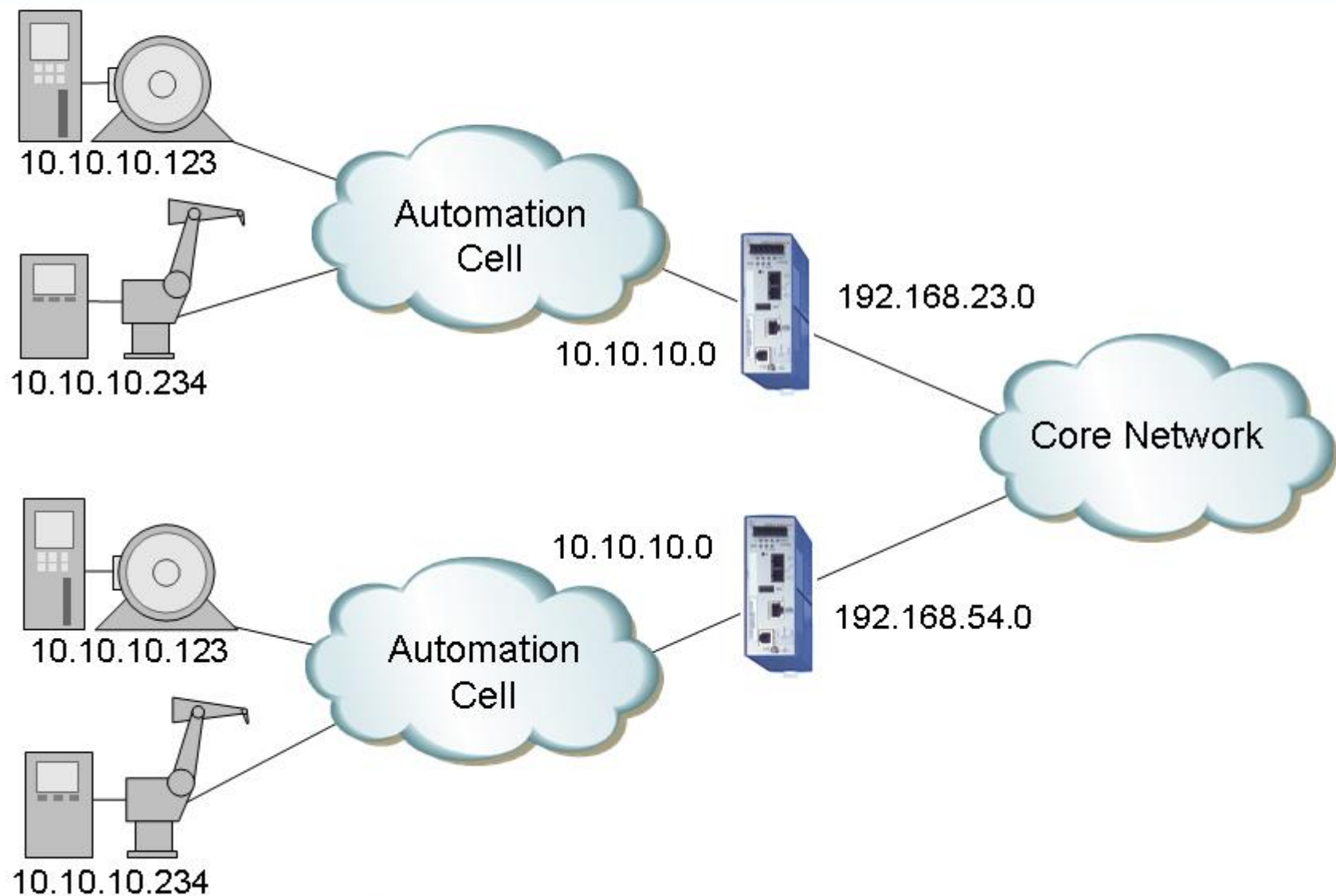
- 网络地址转换 1 to n / 端口地址转换
  - 所有的内部IP地址都映射到唯一的外部IP地址
  - 保护了内部受保护网络的地址结构
  - 通过共享唯一有效的Internet地址从而降低了开支
- 网络地址转换 1 to 1
  - 每个内部地址都映射到各自对应的外部地址
  - 在保护内部网络地址架构的同时实现了有外向内连接的可能

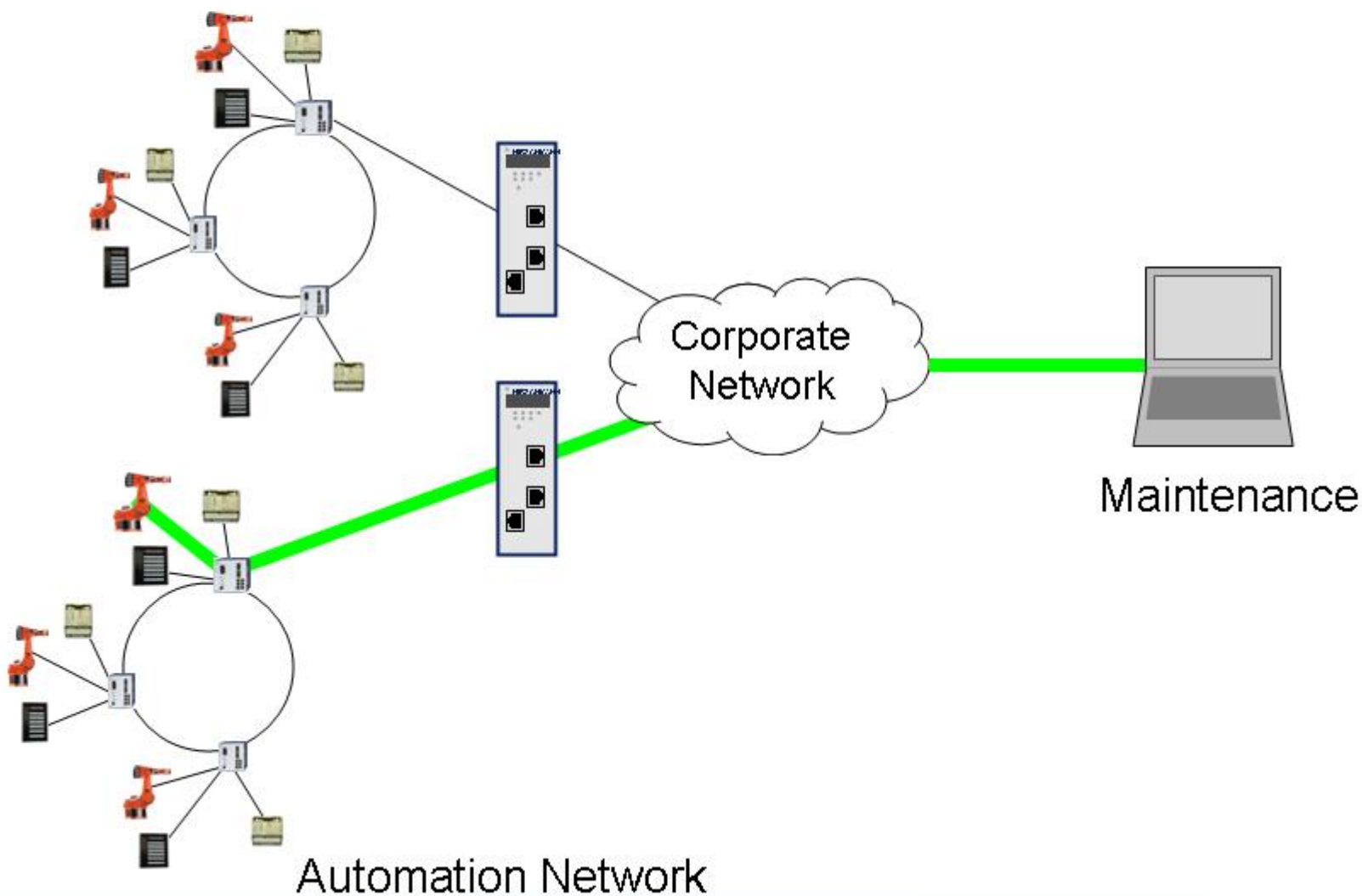
- 映射多个内部地址到唯一的外部IP地址



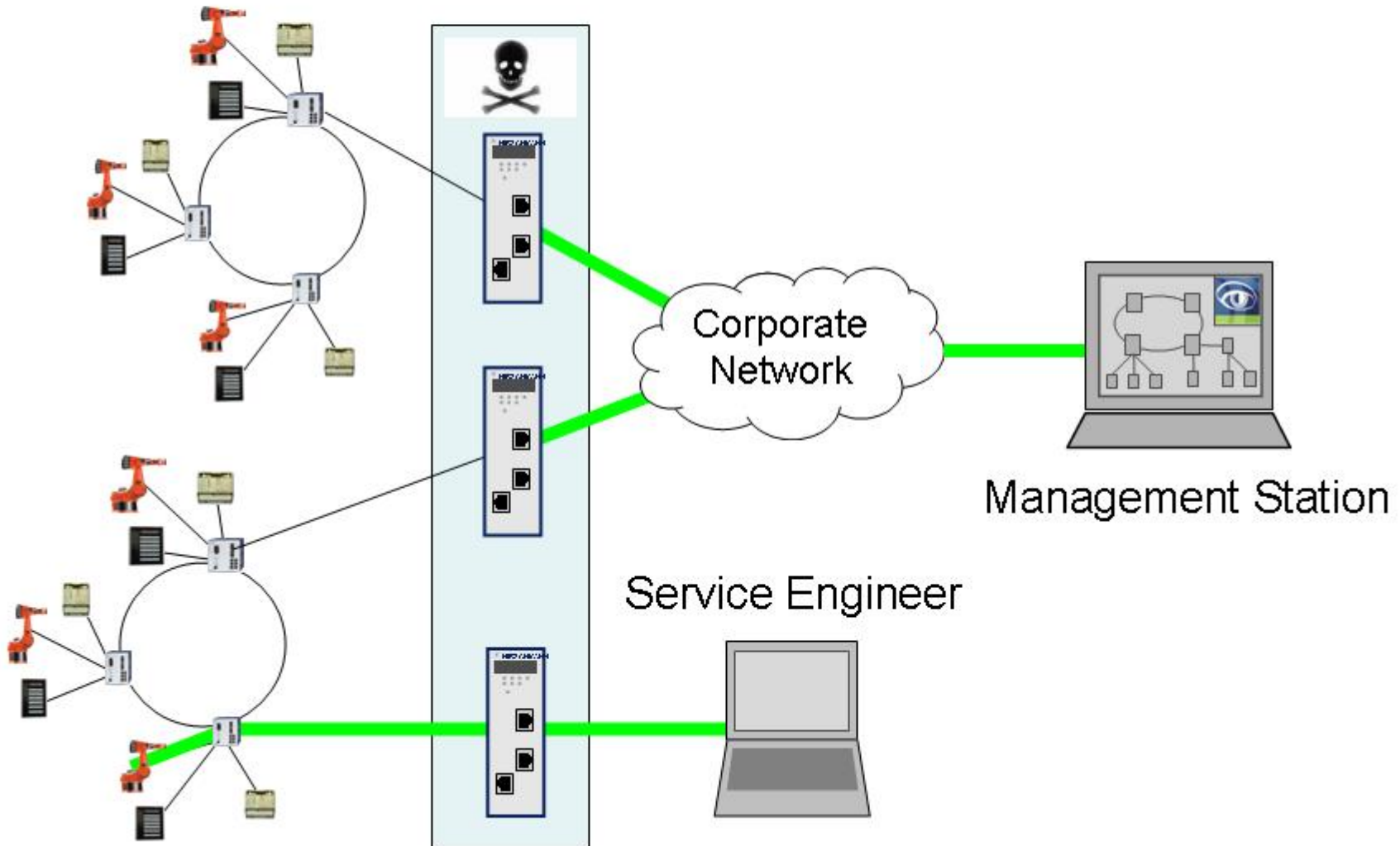
- 内部地址和外部地址之间的 1 to 1 转换.











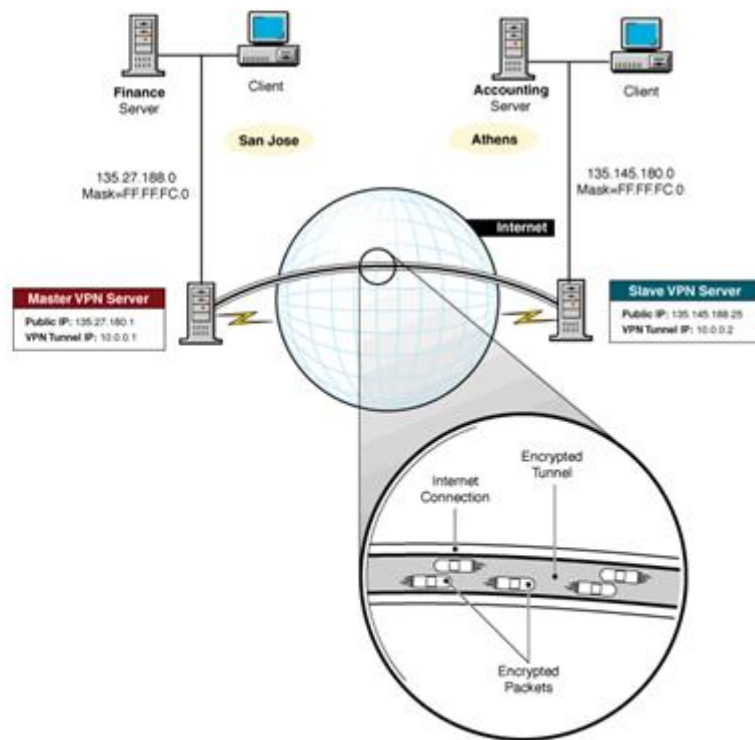


**HIRSCHMANN**

A **BELDEN** BRAND

# 虚拟私有网络VPN

- 虚拟私有网络 (VPN) 是在两点之间跨越非安全网络时建立的一个安全的、加密的连接
- 通过加密和封装IP数据包，信息在一个安全的“隧道”中传递



- Client to Site (C2S) 客户端 – 站点
- 连接单独的PC到一个网络 – 例如，移动办公者
- C2S 的连接通常都是临时的
- 要求：
  - VPN 客户端软件 (IPSec-VPN)
  - Windows集成的VPN连接工具 (PPTP-VPN)
  - 合适的WEB浏览器 (SSL-VPN)



- Site to Site (S2S) 站点 – 站点
- 连接两个网络，例如：
  - 两个分公司之间
  - 透过企业网络的两个工业网络之间
- S2S 的连接通常是永久的 (24x7)



- 优点
  - 具备长远的发展前景
  - 相对比较低的实现开销
  - 可以使用它来构建复杂的网络
  - 加密机制确保了信息的机密性、完整性和可用性
- 缺点
  - 配置和维护复杂

- 硬件的优点：
  - 对终端设备来说不会损失性能
  - 终端设备上也无需安装VPN软件
  - 可选是否带病毒扫描功能



Portable



DIN Rail



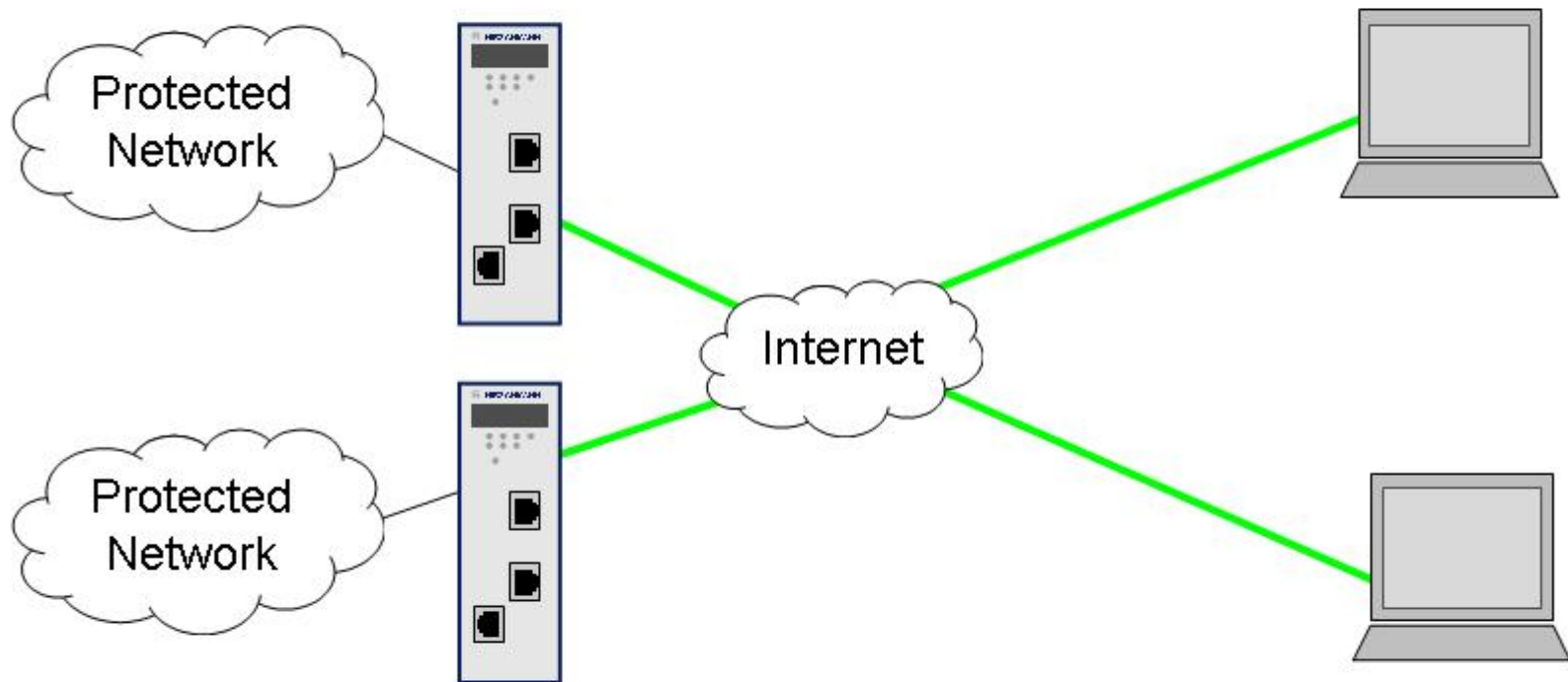
LAN



PCI

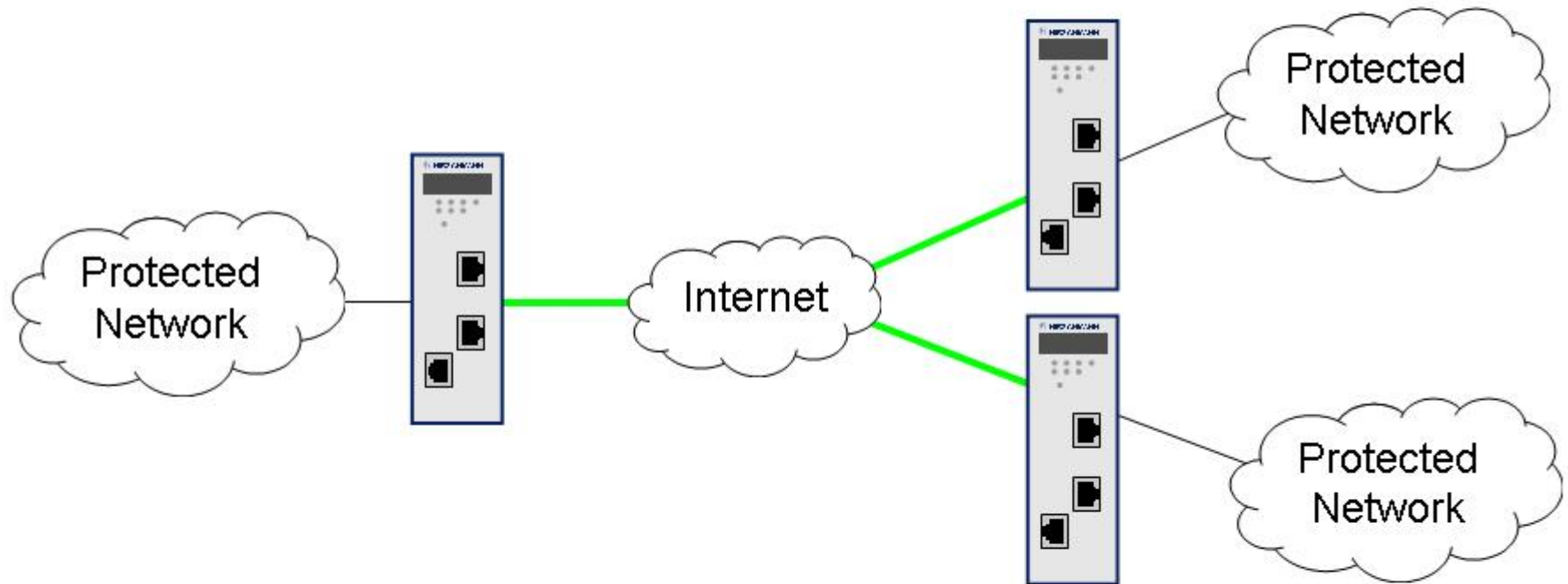


Blade

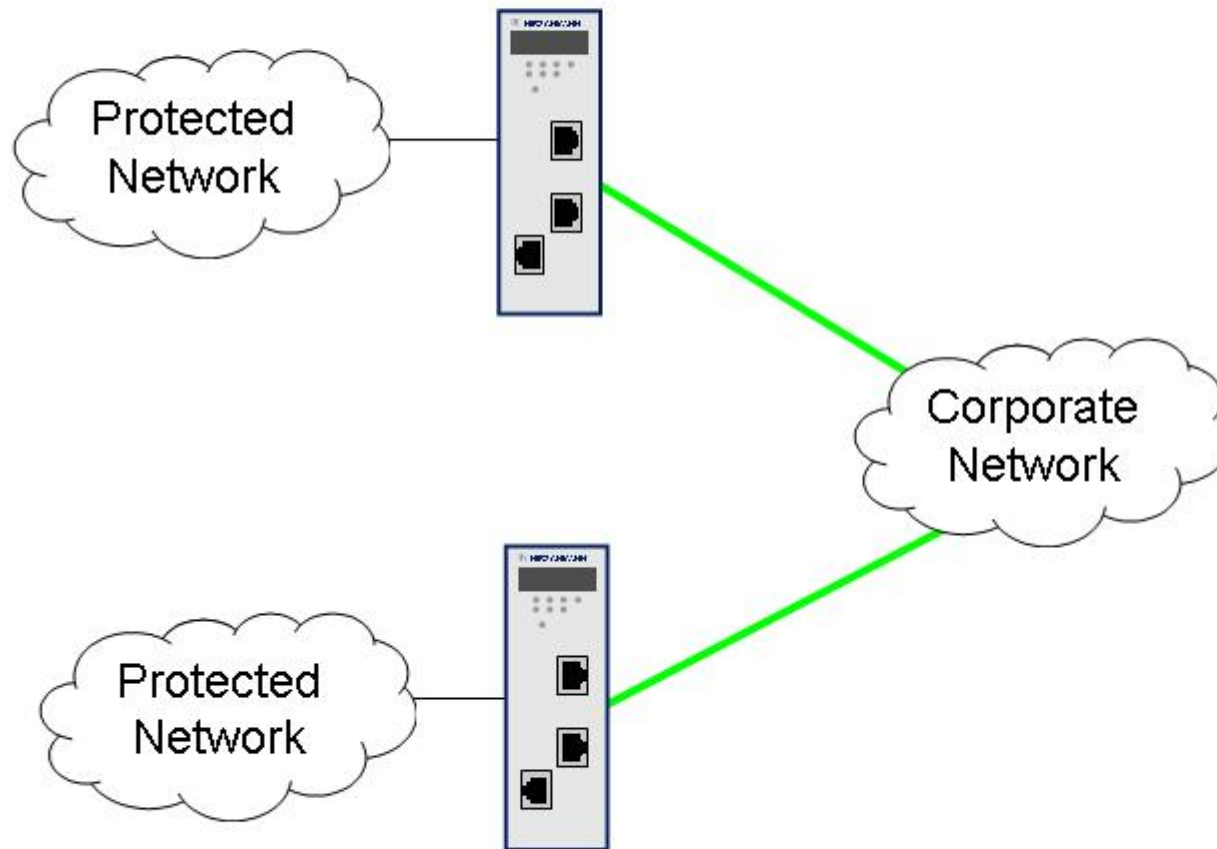


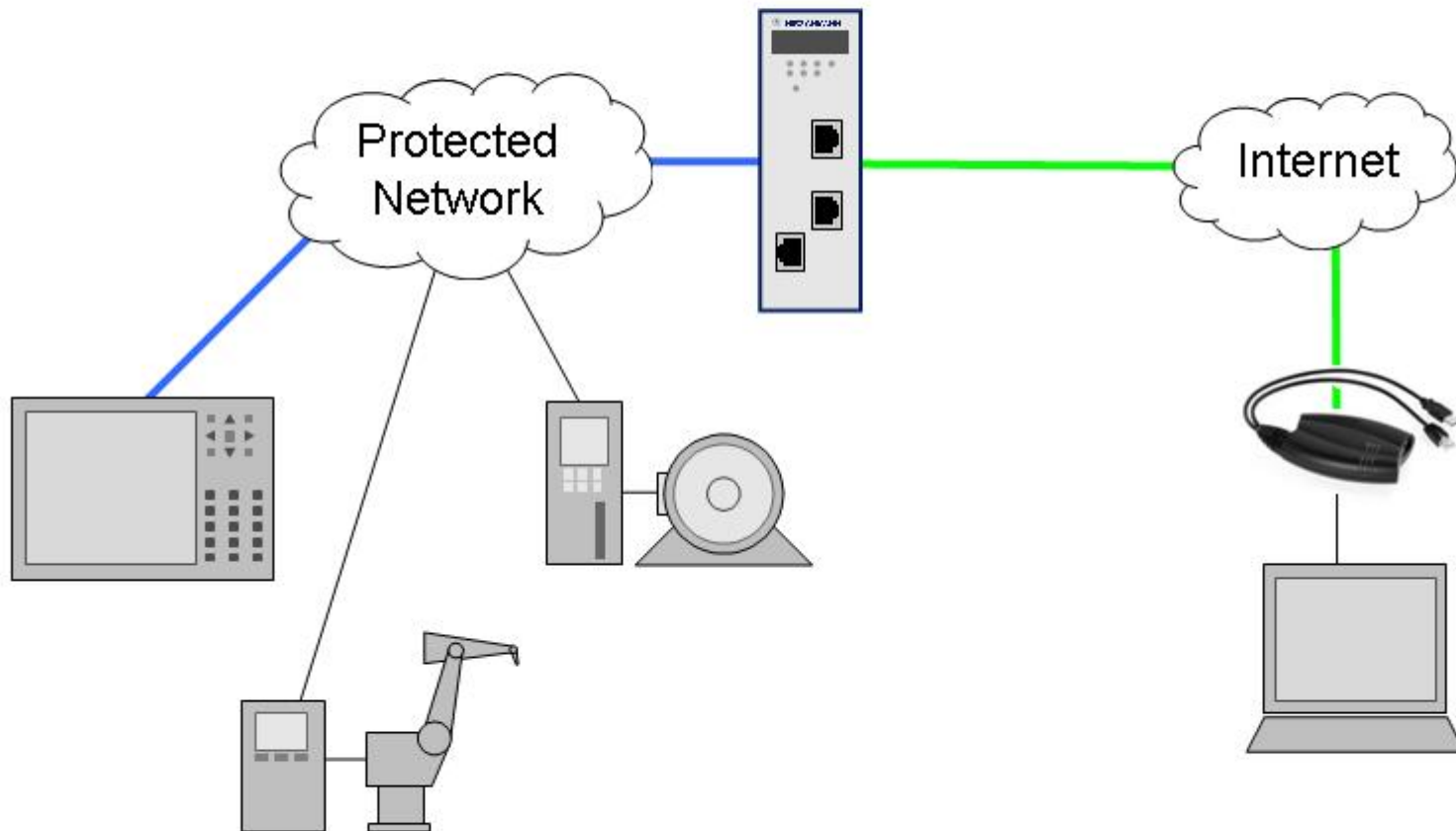


# Connecting Remote Networks



# Creating a VPN over the corporate LAN







**HIRSCHMANN**

A **BELDEN** BRAND

# 结论

- 从一开始设计时就应考虑网络安全因素
- 可网管交换机提供了一系列安全功能
- 控制网络和其它网络互联时必须通过防火墙
- 通过公网连接分支公司时，应使用VPNs
- 成功的安全保护需要一系列的技术支持