

Private VLANs

Autor: Morris Tichy, Lukas Freudensprung

Inhaltsverzeichnis

1. Theorie	2
2. Konzept	2
3. Konfiguration	2
3.1. SW-Sans	2
4. Test	4

1. Theorie

Ein Private VLAN erweitert normale VLANs, indem es den Datenverkehr zwischen bestimmten Ports einschränkt. Es gibt drei Haupttypen von PVLAN-Ports: Promiscuous, Community und Isolated. Der Promiscuous Port kann mit allen anderen PVLAN-Ports kommunizieren (z. B. ein Gateway oder Router). Community Ports können untereinander und mit dem Promiscuous Port kommunizieren, aber nicht mit Isolated Ports oder anderen Community Groups. Isolated Ports dürfen nur mit dem Promiscuous Port kommunizieren, nicht untereinander oder mit Community Ports. Das erhöht die Sicherheit, indem bestimmte Geräte voneinander getrennt bleiben.

2. Konzept

In dem Standort Sanctum Sanctorum gibt es einen RODC und einen Client (VPCS). Diese sind durch Private Isolated VLANs von einander getrennt und kommen daher nur zu ihrem Gateway, der pfSense, über den Promiscuous Port.

3. Konfiguration

3.1. SW-Sans

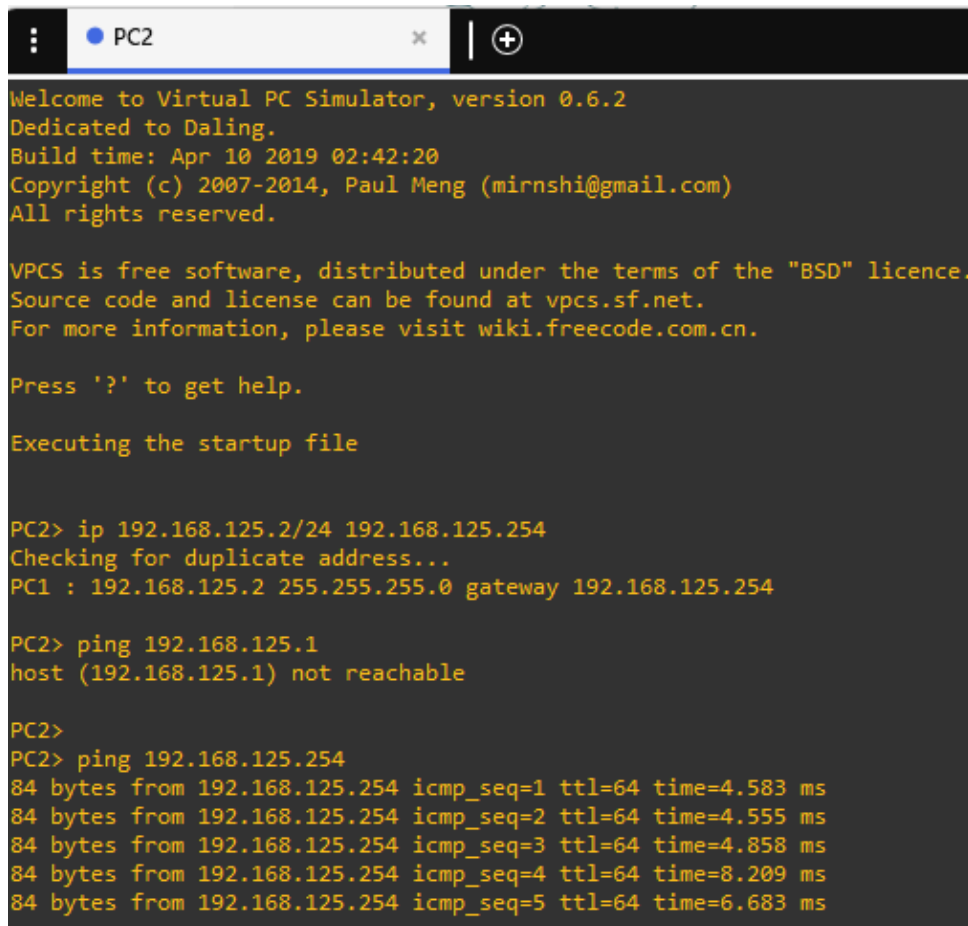
```
1  # Konfiguration des Switches und der Private VLANs
2
3  en
4  conf t
5  ho SW-SanS
6  no ip domain-lookup
7  usern cisco priv 15
8  usern cisco al sc se cisco
9  ip domain-name 5CN
10 crypto key ge rsa us m 1024
11 ip ssh v 2
12
13 line vty 0 924
14 transport input ssh
15 login local
16 exit
```

[shell](#)

```
17
18 line con 0
19 exec-time 0 0
20 exit
21
22 vtp mode transparent
23
24 # Private Isolated VLAN erstellen
25 vlan 100
26 name isolated-vlan-100
27 private-vlan isolated
28 exit
29
30 # Primary VLAN erstellen
31 vlan 10
32 name primary-vlan-10
33 private-vlan primary
34 private-vlan association add 100
35 exit
36
37 # Promiscuous Port konfigurieren
38 int gi0/0
39 des T0_pfsense2
40 switchport mode private-vlan promiscuous
41 switchport private-vlan mapping 10 100
42 exit
43
44 # Isolated Ports konfigurieren
45 int gi0/1
46 des T0_R0DC
47 switchport mode private-vlan host
48 switchport private-vlan host-association 10 100
49 exit
50
51 int gi0/2
52 des T0_PC2
53 switchport mode private-vlan host
54 switchport private-vlan host-association 10 100
55 exit
```

4. Test

In folgendem Screenshot ist zu sehen, wie PC2 versucht den RODC mit der IP Adresse 192.168.125.1 zu erreichen. Da PC2 nur mit dem Promiscuous Port kommunizieren darf kann er nur die IP Adresse 192.168.125.254 (pfsense) pingen.



```
PC2
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip 192.168.125.2/24 192.168.125.254
Checking for duplicate address...
PC1 : 192.168.125.2 255.255.255.0 gateway 192.168.125.254

PC2> ping 192.168.125.1
host (192.168.125.1) not reachable

PC2>
PC2> ping 192.168.125.254
84 bytes from 192.168.125.254 icmp_seq=1 ttl=64 time=4.583 ms
84 bytes from 192.168.125.254 icmp_seq=2 ttl=64 time=4.555 ms
84 bytes from 192.168.125.254 icmp_seq=3 ttl=64 time=4.858 ms
84 bytes from 192.168.125.254 icmp_seq=4 ttl=64 time=8.209 ms
84 bytes from 192.168.125.254 icmp_seq=5 ttl=64 time=6.683 ms
```

Abbildung 1: Test Ping von PC2