



ASA & Clean Access (Firewall & VPN- SSO with CCA)

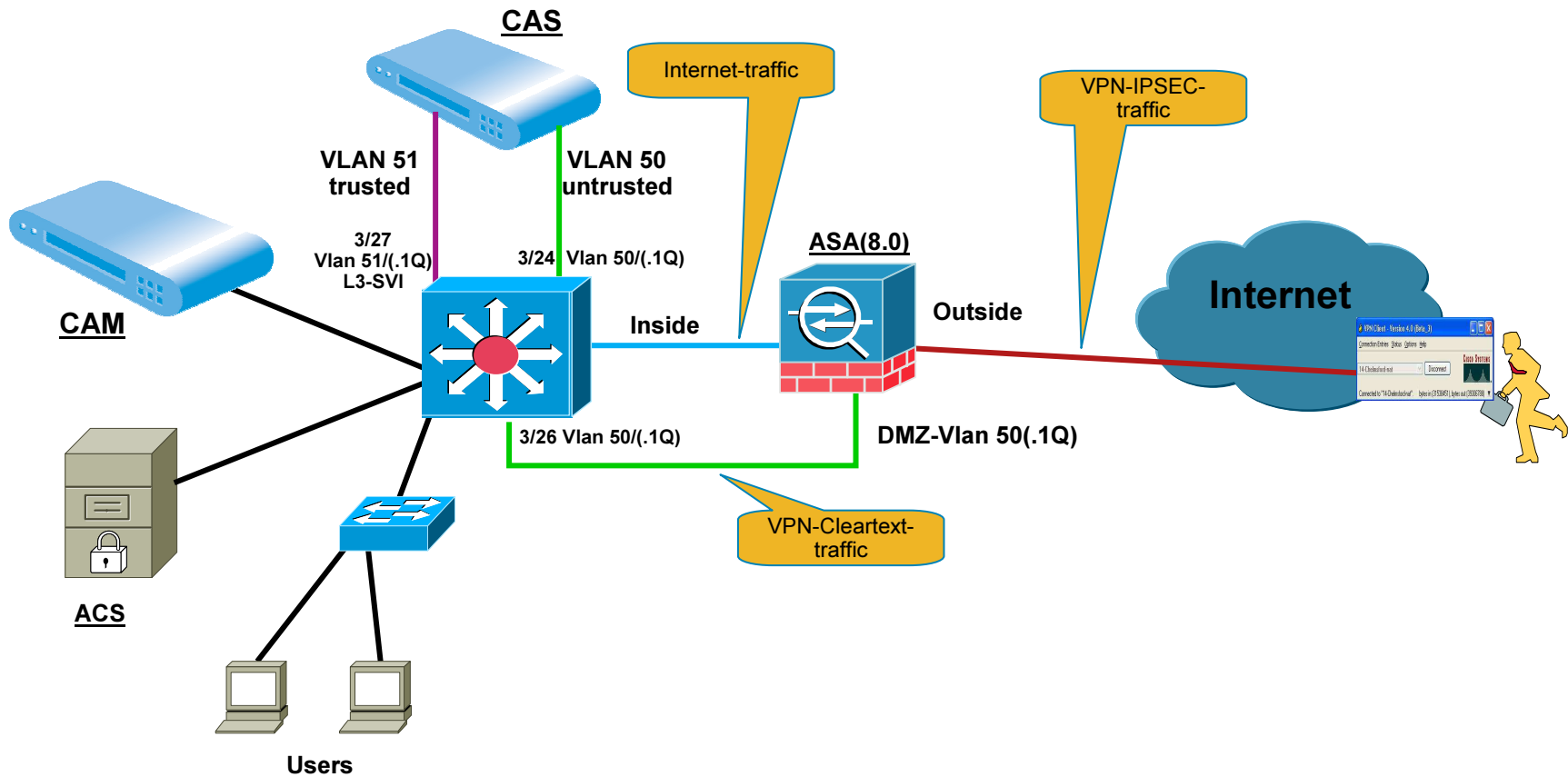


Michael Vassigh

Challenge

- Use single ASA for RAS-VPN & Clean Access & Internetfirewall
- CAS sits “Inband, L2 Virtual GW” behind ASA
- ASA does not support PBR
- regular Internettraffic must not pass CAS (no statefulness etc.)

Network drawing



Solution Suggestion

- Use ASA 8.0 Software
- Use ASA DMZ-Interface with VLAN-Tag
- Limit VPN-Clear-Text Traffic to VLAN
- Use Tunnel-Gateway to direct traffic through CAS
- MAP “Group-Policy” to VLAN
- Keep VPN-SSO feature for CCA-Agent

ASA-Config samples(1)

Configure ASA DMZ VLAN interface:

interface Ethernet0/2.50 (<= this is the dot1Q VLAN Subinterface)

vlan 50

nameif dmz-vlan

security-level 80

ip address 10.1.50.2 255.255.255.0

(we use a Static-Route on the switch, for the VPN-Pool Subnet, to point to the ASA)

ASA VPN Group-Policy configuration mapping into VLAN-50:

group-policy *Trusted* attributes

vpn-simultaneous-logins 1

vpn-idle-timeout 10

vpn-tunnel-protocol IPSec svc webvpn

secure-unit-authentication enable

user-authentication enable

vlan 50 (<= here we limit/forward the traffic to the VLAN)

address-pools value IPSecPool

ASA Tunnel-Group (references Group-Policy & Accounting info):

tunnel-group RA general-attributes

address-pool IPSecPool

authentication-server-group ACS LOCAL

accounting-server-group *CAS-Accounting*

default-group-policy *Trusted*

Static-Route to forward VPN-traffic towards CAS:

route dmz-vlan 0.0.0.0 0.0.0.0 **10.1.50.1** tunneled (this is the special route for the tunneled traffic)

Route inside 10.10.20.0 255.255.255.0 10.10.10.1 (**More specific route not preferred by vlan tag VPN traffic**)

(10.1.50.1 = Switch SVI-Interface, acting as L3 GW for „bridged CAS traffic)

ASA-Config samples(2)

CAS-VPN-SSO configuration (for ASA Accounting records):

```
aaa-server CAS-Accounting protocol radius
aaa-server CAS-Accounting (dmz-vlan) host 10.1.50.5 (<=IP Adress of CAS trusted interface)
key cisco123
authentication-port 1812
accounting-port 1813
radius-common-pw cisco123
```

Switch-Config samples(1)

CAS-untrusted interface on Switch:

```
interface FastEthernet3/24
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50
switchport mode trunk
spanning-tree portfast
```

CAS-trusted interface on Switch:

```
interface FastEthernet3/27
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 51
switchport mode trunk
```

ASA-Trunk Interface on Switch

```
interface FastEthernet3/26
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50
switchport mode trunk
```

Switch-L3 Interface

```
interface Vlan51
ip address 10.1.50.1 255.255.255.0
```

Route VPN return-traffic to ASA-Interface (10.1.70.x = VPN-Pool Subnet)

```
ip route 10.1.70.0 255.255.255.0 10.1.50.2
```

How Routing is done for VPN (VLAN) Traffic

- The VPN traffic (**With VLAN Tag**) will only look for the tunnel default gateway pointing to the exit interface (DMZ VLAN interface) in the same VLAN
- VPN Traffic (**Without VLAN tag**) will look at the routing table and more specific route will be preferred over tunnel default gateway
- The return traffic (**Non-VPN**) for inside users will look up the normal routing table to decide the exit interface (inside interface)

- Show Route on ASA:

```
S 10.10.20.0 255.255.255.0 [1/0] via 10.10.10.1, inside
```

```
S 0.0.0.0 0.0.0.0 [255/0] via 10.10.50.1, DMZ-VPN tunneled
```

VLAN tag VPN traffic will only use the tunnel default gateway

