Cisco TrustSec

Software Defined Segmentation
Segurança e Mobilidade

Wilson Rogério Lopes

GTS 27

05/2016

Cisco TrustSec

- Segregação e controle de acesso, independente de ip e vlan
- Security Group Policies

  Usuários ou dispositivos são classificados e associados à um Security Group, identificados por um Security Group Tag
- Administração e distribuição centralizada das políticas

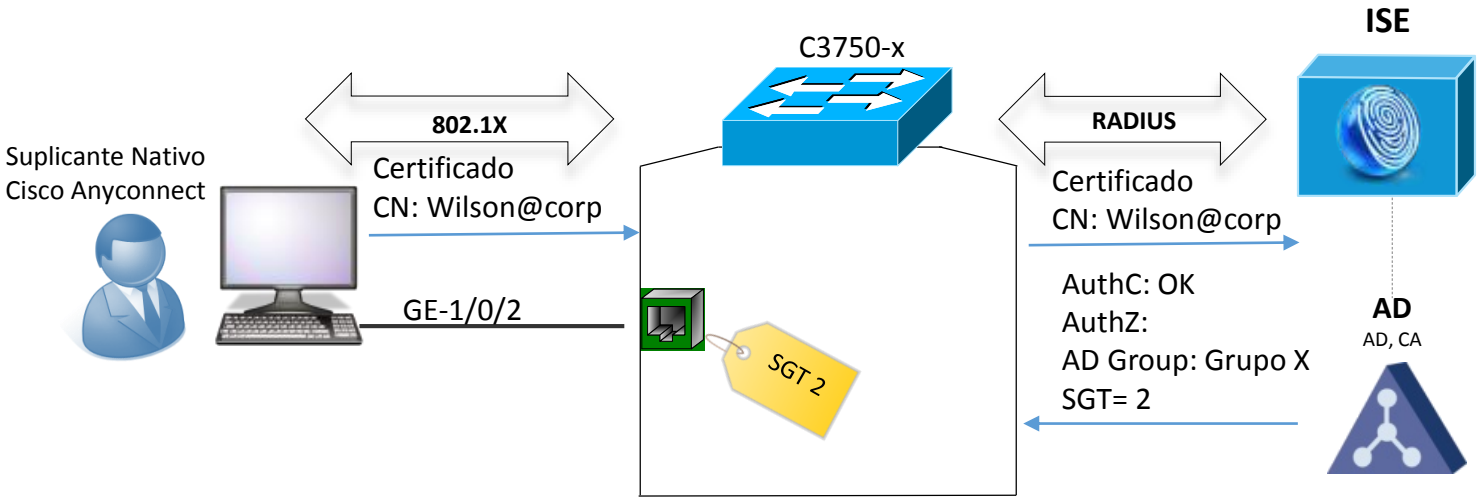
ISE – Identity Services Engine

AD, LDAP

- Radius Server
- Políticas Centralizadas
- AAA Services
- Verificação de postura
- Profiling de dispositivos
- Monitoração
- Relatórios

SGT – Security Group Tag

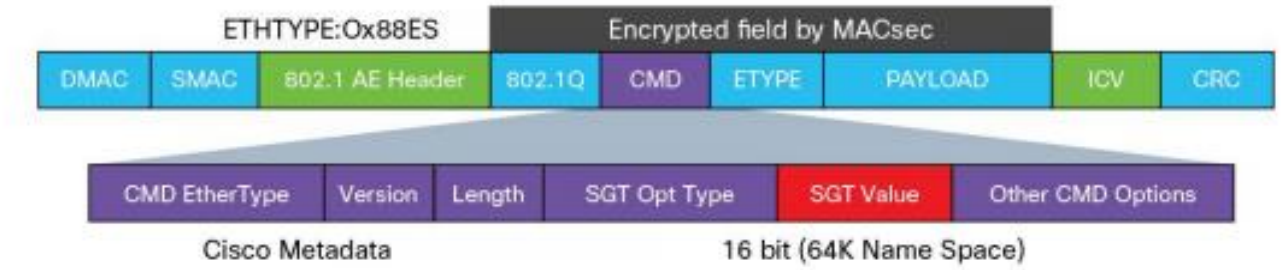
- 16 bits = 65536 SGTs possíveis
- TAG inserido no frame ethernet na entrada da rede
- Associação dinâmica – 802.1x, MAB, Profiling



SGT – Security Group Tag

- Associação Estática
  - IP to SGT

DEV/Homolog Servers SGT 10	ERP Servers SGT 20	Mail Servers SGT 30	Proxy Servers SGT 40
10.200.0.10 10.20.0.11 10.10.0.10	10.100.0.10 10.100.0.11 10.50.0.10	10.101.0.10 10.101.0.11 10.60.0.10	10.200.0.10 10.200.0.11



* Associação de SGT requer suporte em hardware

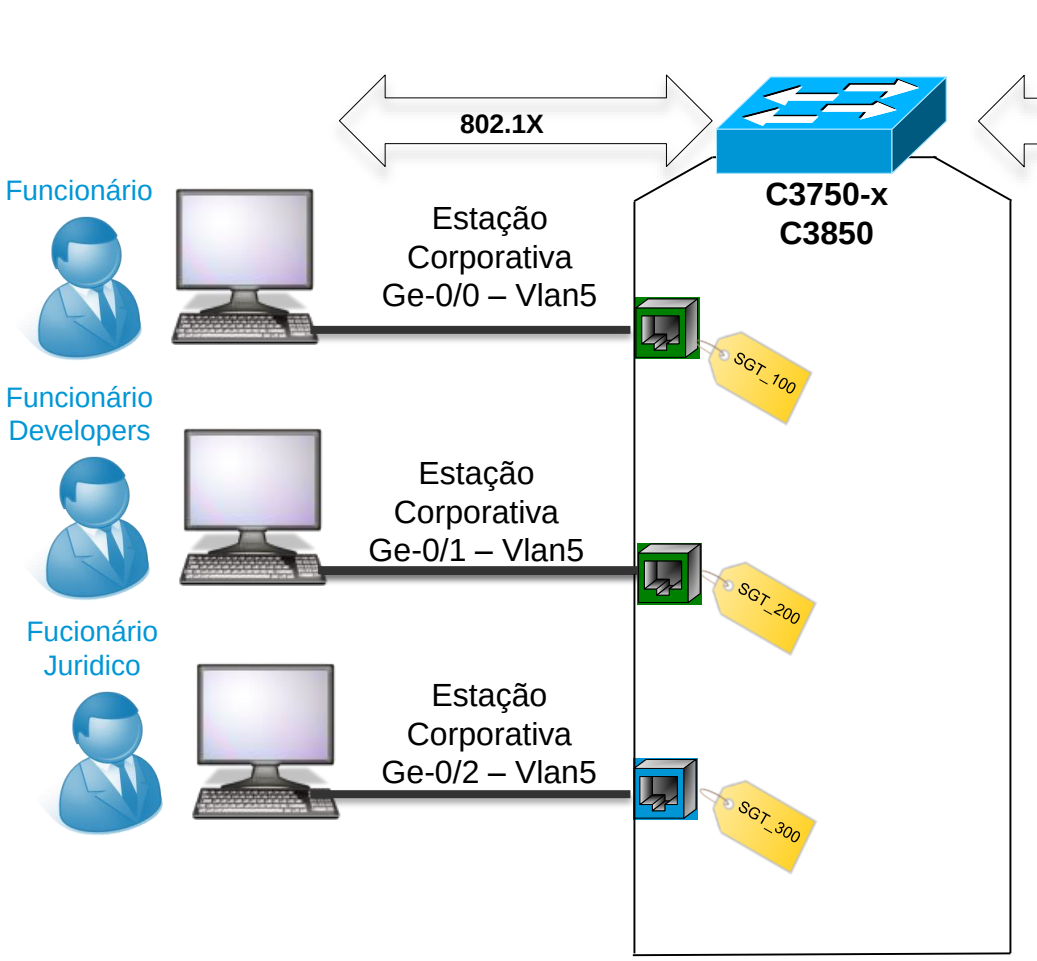
SGACL – Security Group ACL

- ACL baseada em SGT de origem x SGT de destino
- Matriz de acesso
- Default permit

Origem / Destino	**Funcionário**	**Developer**	**Juridico**
Funcionário	SGACL-A	SGACL-A	SGACL-A
Developer	SGACL-A	SGACL-B	SGACL-A
Jurídico	SGACL-A	SGACL-A	SGACL-A

Use Case - Bloqueio User to User

- **Malwares e APTs – ploriferação lateral**
- **Acesso RDP não autorizado**



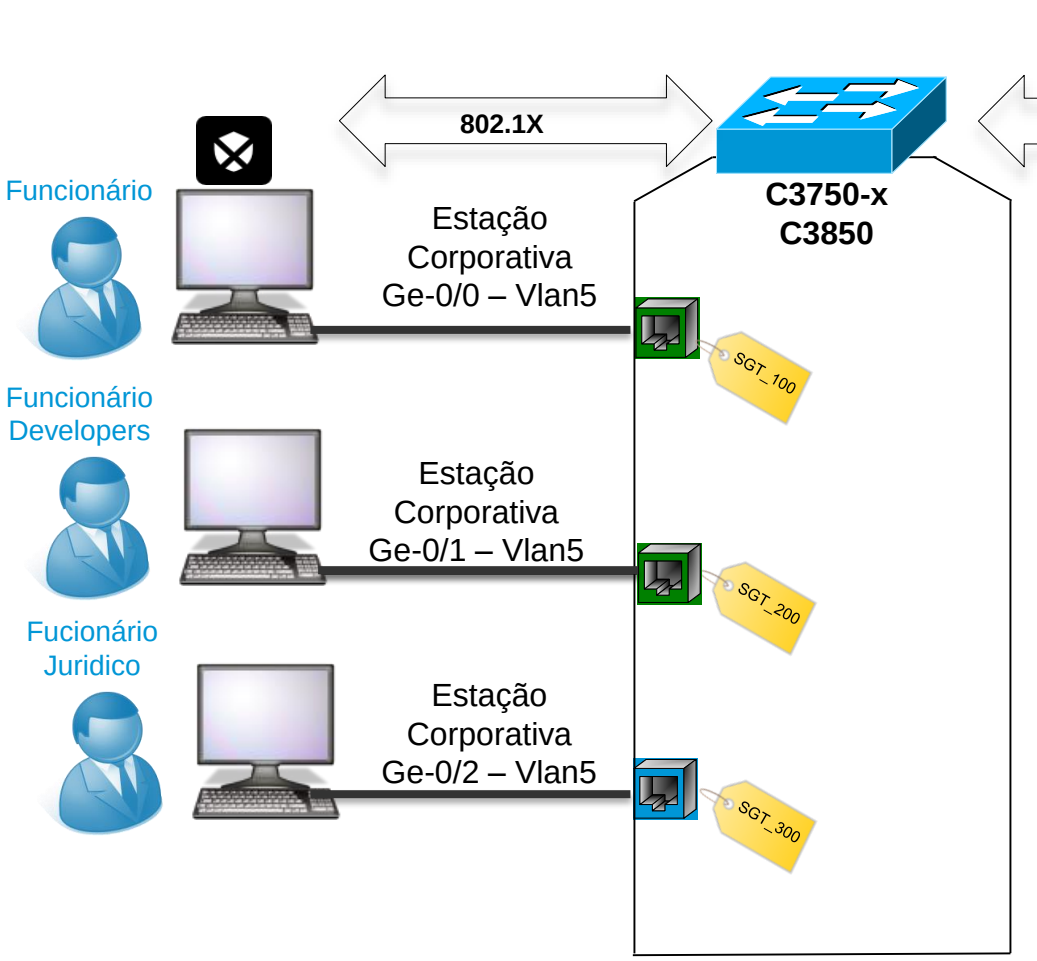
Origem / Destino	**Funcionário**	**Developer**	**Juridico**
Funcionário	SGACL-A	SGACL-A	SGACL-A
Developer	SGACL-A	SGACL-B	SGACL-A
Jurídico	SGACL-A	SGACL-A	SGACL-A

SGACL-A
Deny ip

SGACL-B
Permit tcp dst eq 80 **Permit tcp dst eq 443** **Permit tcp dst eq 8080** **Deny ip**

Use Case - Bloqueio User to User

- **Malwares e APTs – ploriferação lateral**
- **Acesso RDP não autorizado**



Origem / Destino	Funcionário	Developer	Juridico
Funcionário	SGACL-A	SGACL-A	SGACL-A
Developer	SGACL-A	SGACL-B	SGACL-A
Jurídico	SGACL-A	SGACL-A	SGACL-A

SGACL-A

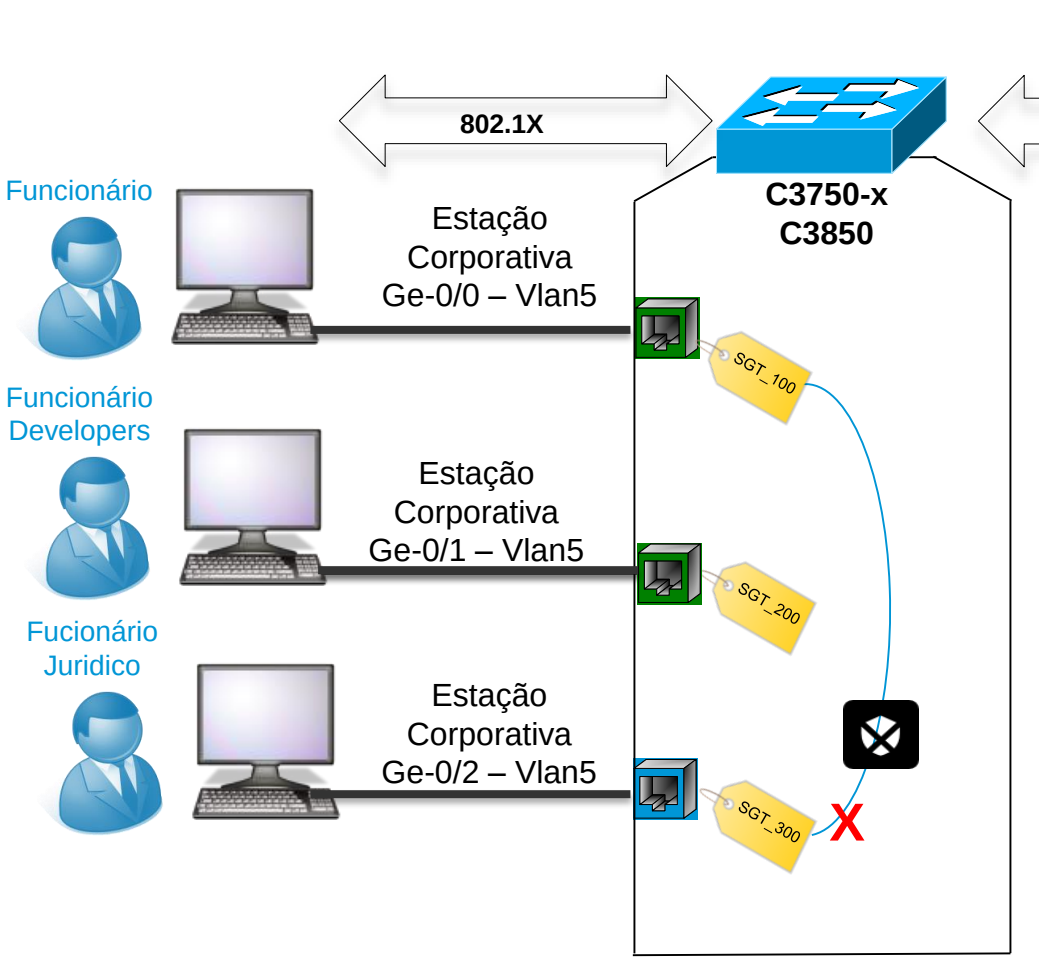
Deny ip

SGACL-B

Permit tcp dst eq 80
Permit tcp dst eq 443
Permit tcp dst eq 8080
Deny ip

Use Case - Bloqueio User to User

- **Malwares e APTs – ploriferação lateral**
- **Acesso RDP não autorizado**

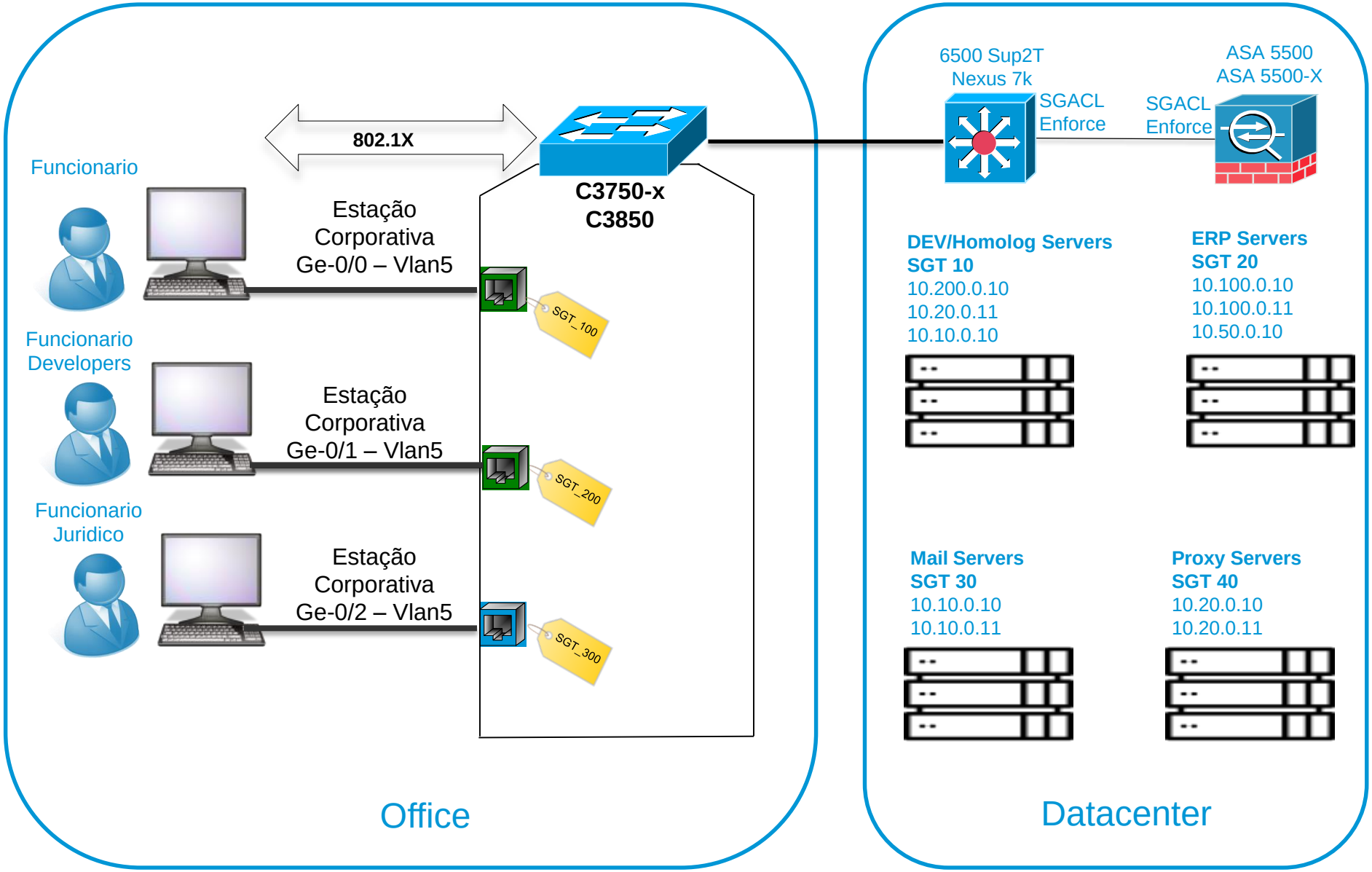


Origem / Destino	Funcionário	Developer	Juridico
Funcionário	SGACL-A	SGACL-A	SGACL-A
Developer	SGACL-A	SGACL-B	SGACL-A
Jurídico	SGACL-A	SGACL-A	SGACL-A

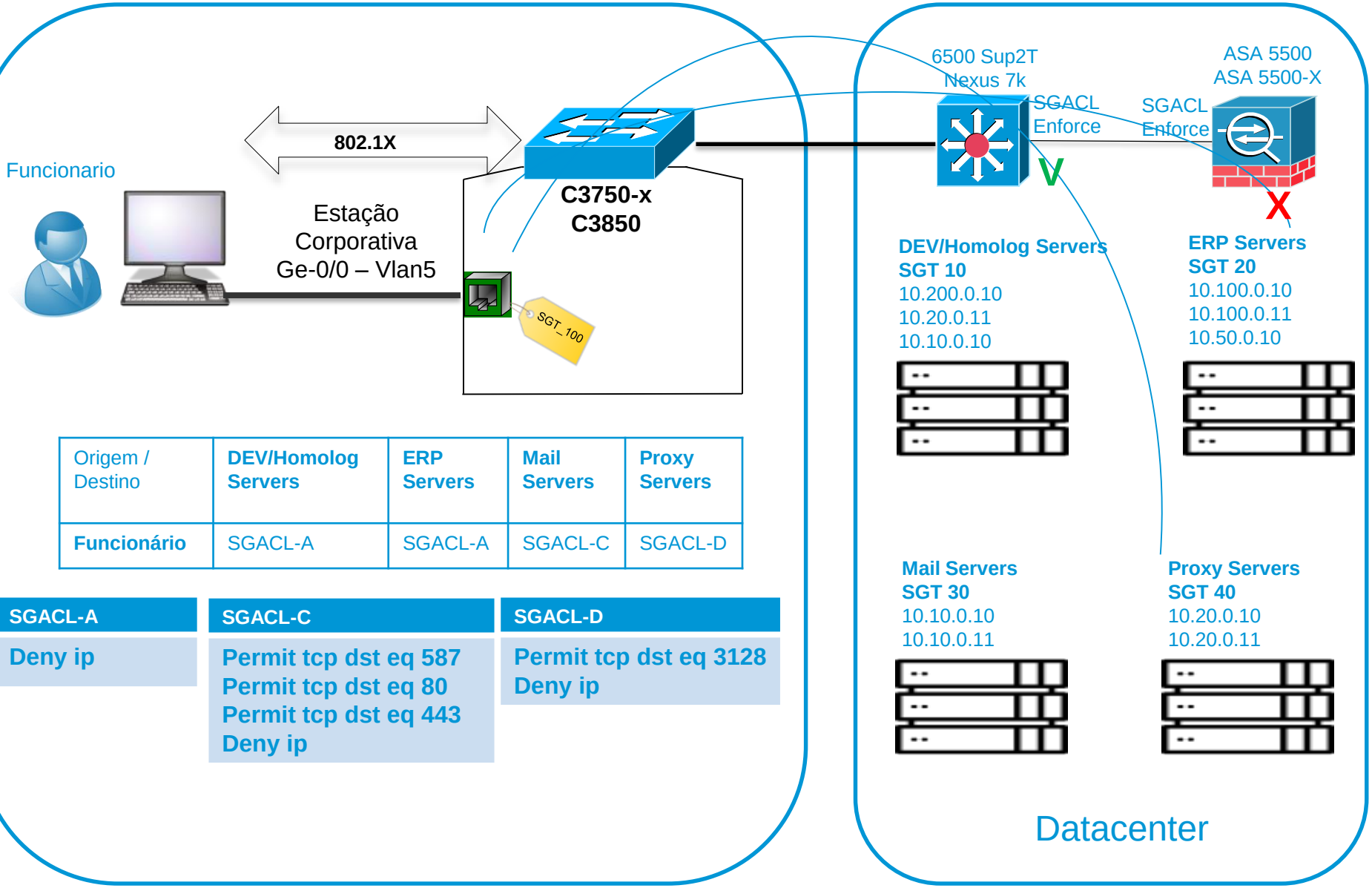
SGACL-A
Deny ip

SGACL-B
Permit tcp dst eq 80 Permit tcp dst eq 443 Permit tcp dst eq 8080 Deny ip

Use Case - Bloqueio User do DC



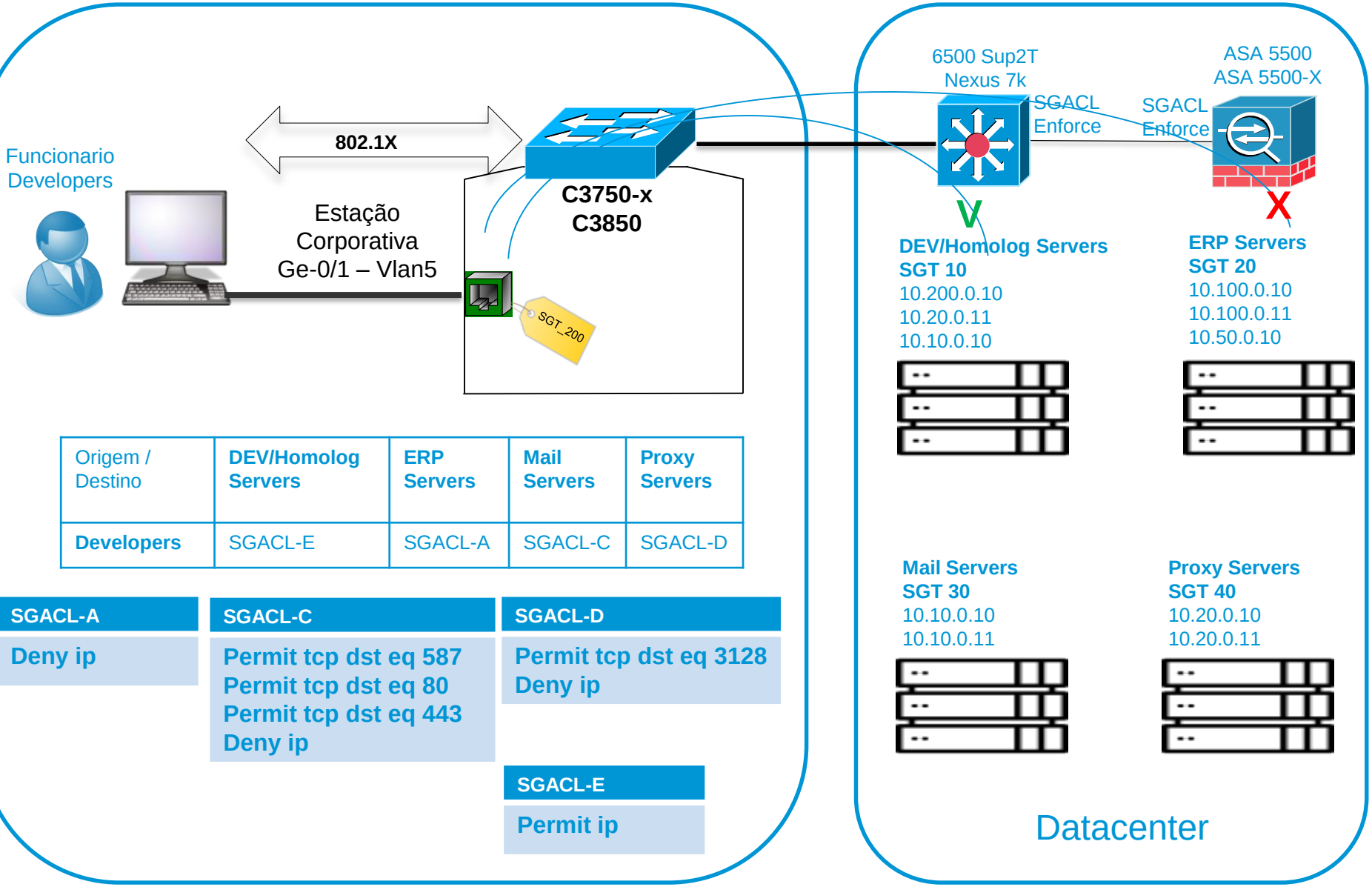
Use Case - Bloqueio User do DC



Origem / Destino	DEV/Homolog Servers	ERP Servers	Mail Servers	Proxy Servers
Funcionário	SGACL-A	SGACL-A	SGACL-C	SGACL-D

SGACL-A	SGACL-C	SGACL-D
Deny ip	**Permit tcp dst eq 587** **Permit tcp dst eq 80** **Permit tcp dst eq 443** **Deny ip**	**Permit tcp dst eq 3128** **Deny ip**

Use Case - Bloqueio User do DC



Origem / Destino	DEV/Homolog Servers	ERP Servers	Mail Servers	Proxy Servers
Developers	SGACL-E	SGACL-A	SGACL-C	SGACL-D

SGACL-A

Deny ip

SGACL-C

Permit tcp dst eq 587
Permit tcp dst eq 80
Permit tcp dst eq 443
Deny ip

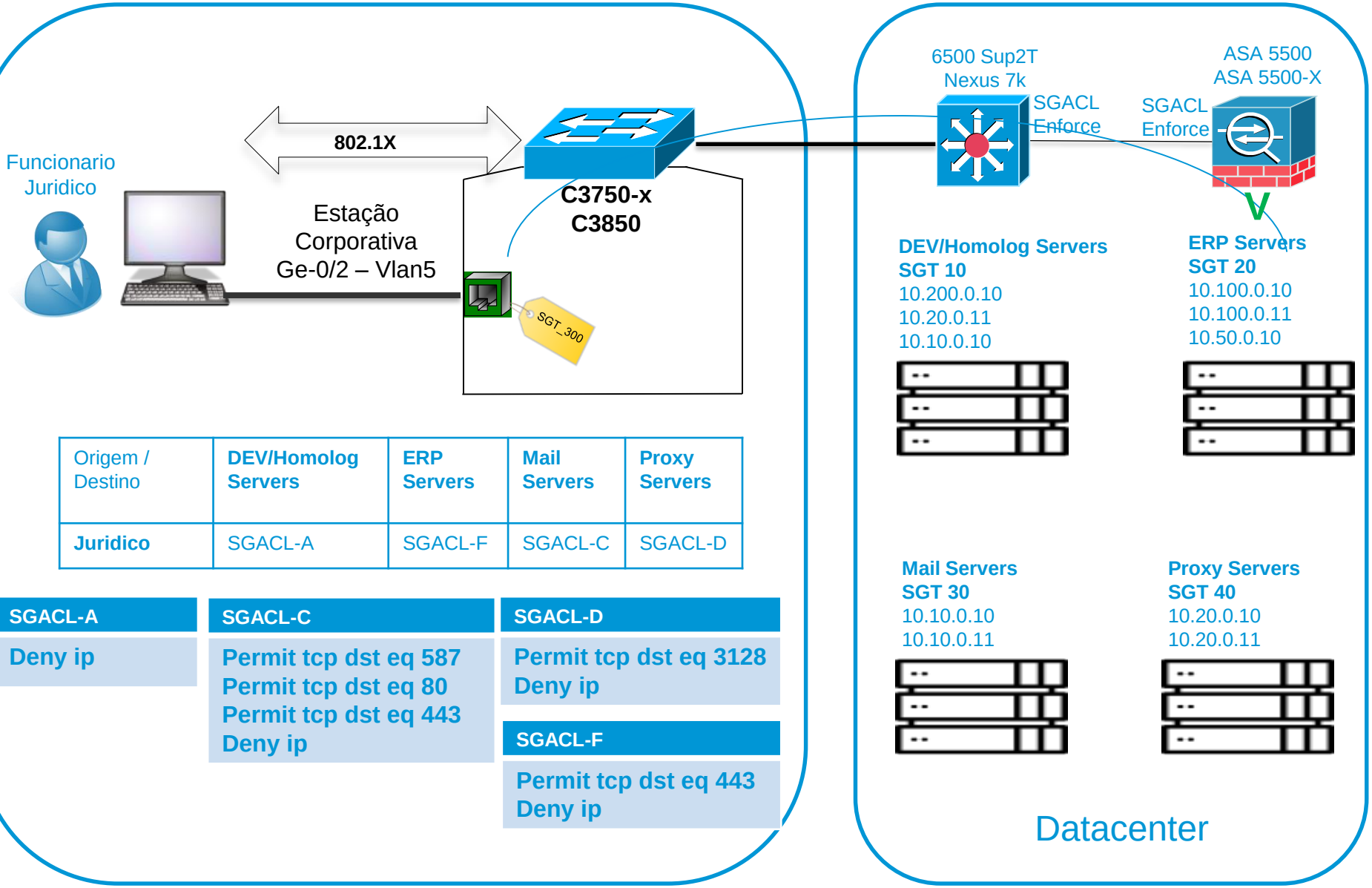
SGACL-D

Permit tcp dst eq 3128
Deny ip

SGACL-E

Permit ip

Use Case - Bloqueio User do DC



Origem / Destino	DEV/Homolog Servers	ERP Servers	Mail Servers	Proxy Servers
Juridico	SGACL-A	SGACL-F	SGACL-C	SGACL-D

SGACL-A

Deny ip

SGACL-C

Permit tcp dst eq 587
Permit tcp dst eq 80
Permit tcp dst eq 443
Deny ip

SGACL-D

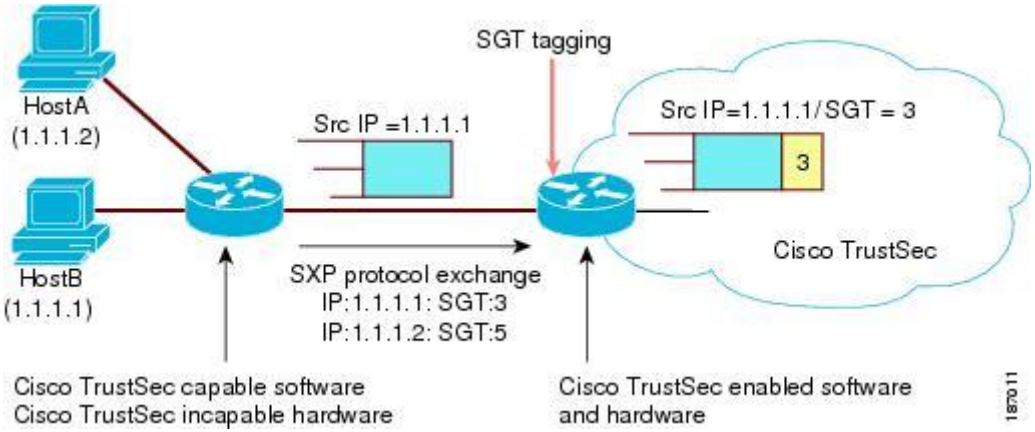
Permit tcp dst eq 3128
Deny ip

SGACL-F

Permit tcp dst eq 443
Deny ip

SXP – SGT Exchange Protocol

- **Propagação IP-to-SGT via software**
- **Protocolo TCP, similar ao BGP**
- **IP Device Tracking ou DHCP Snooping para identificar o ip**
- **Draft IETF - https://tools.ietf.org/html/draft-smith-kandula-sxp-00**



Obrigado ☺

Wilson Rogério Lopes

Áreas de interesse:

Arquitetura de redes
Segurança de redes
Soluções anti-DDoS
NFV, SDN
Puppet

wilsonlopes00@gmail.com

https://br.linkedin.com/in/wrlopes