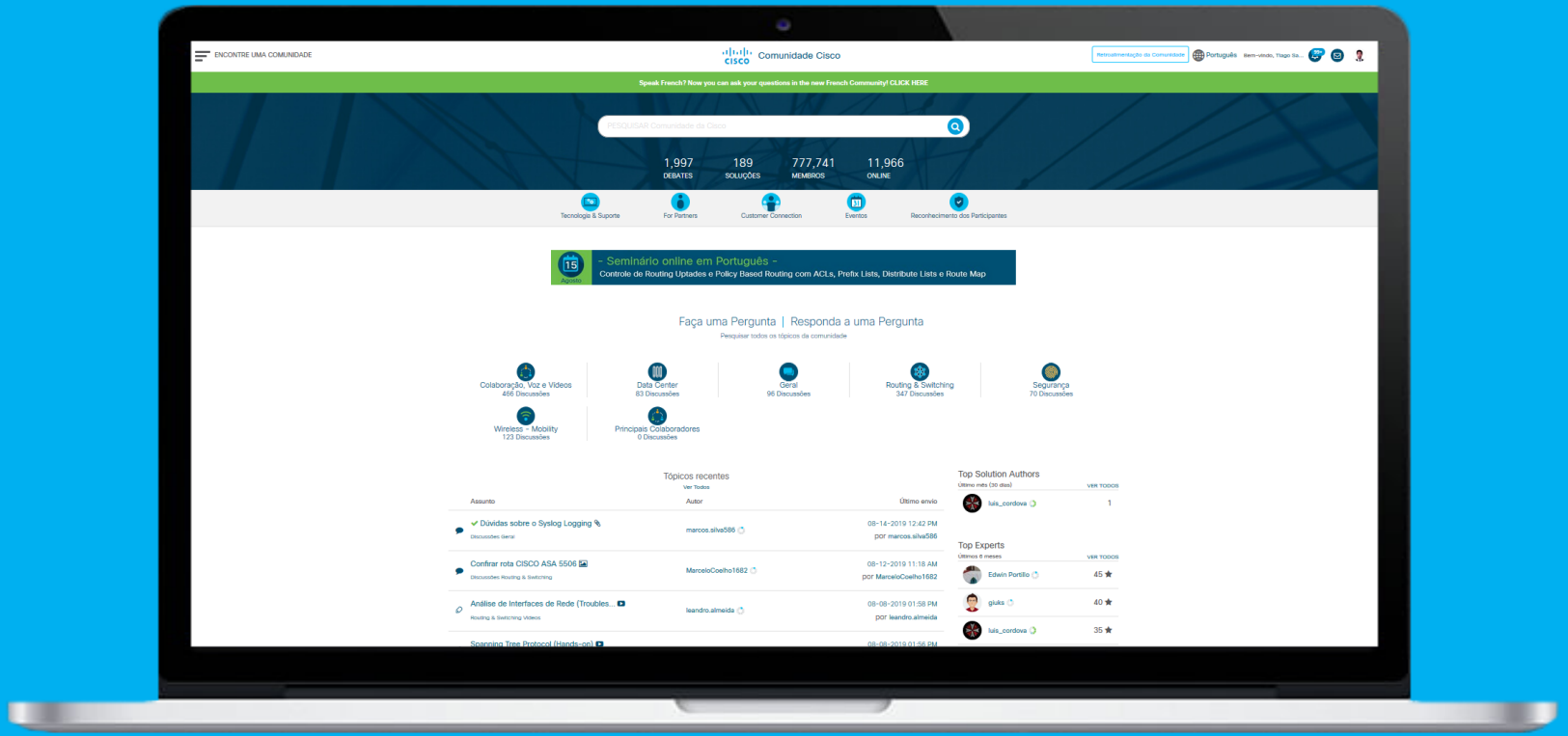
Comunidade Cisco em Português Webcast

Mitigação de ataques em redes de computadores utilizando 802.1X, TrustSec e MacSec

Luis Matos
Arquiteto de Soluções
4 de setembro de 2019



http://community.cisco.com

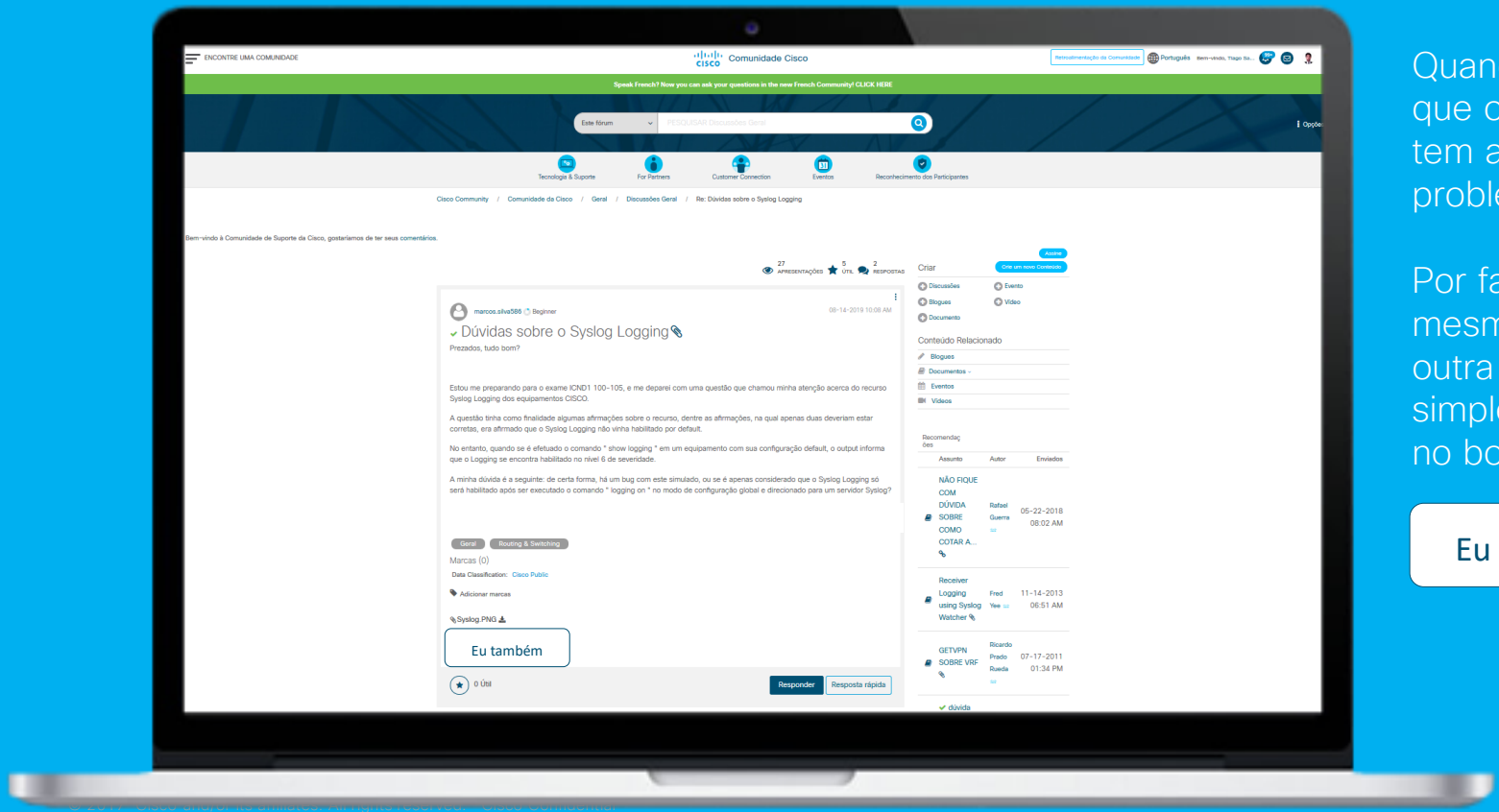
Avalie os conteúdos publicados na Comunidade

Agradeça as pessoas que compartilham generosamente seus conhecimentos dentro da Comunidade dando um Kudo, ou seja, (clicando sobre a estrelinha).

Respostas
Blogs
Documentos
Eventos
Vídeos

Conheça o ranking dos membros com mais Kudos recebidos aqui:
https://community.cisco.com/t5/kudos/kudosleaderboardpage/category-id/comunidade-portugues/timerange/one_month/page/1/tab/authors

Receba respostas ainda mais rápido!



Quando perceber que outra pessoa tem a mesmo problema ou dúvida.

Por favor, não faça a mesma pergunta outra vez, simplesmente clique no botão:

Eu também

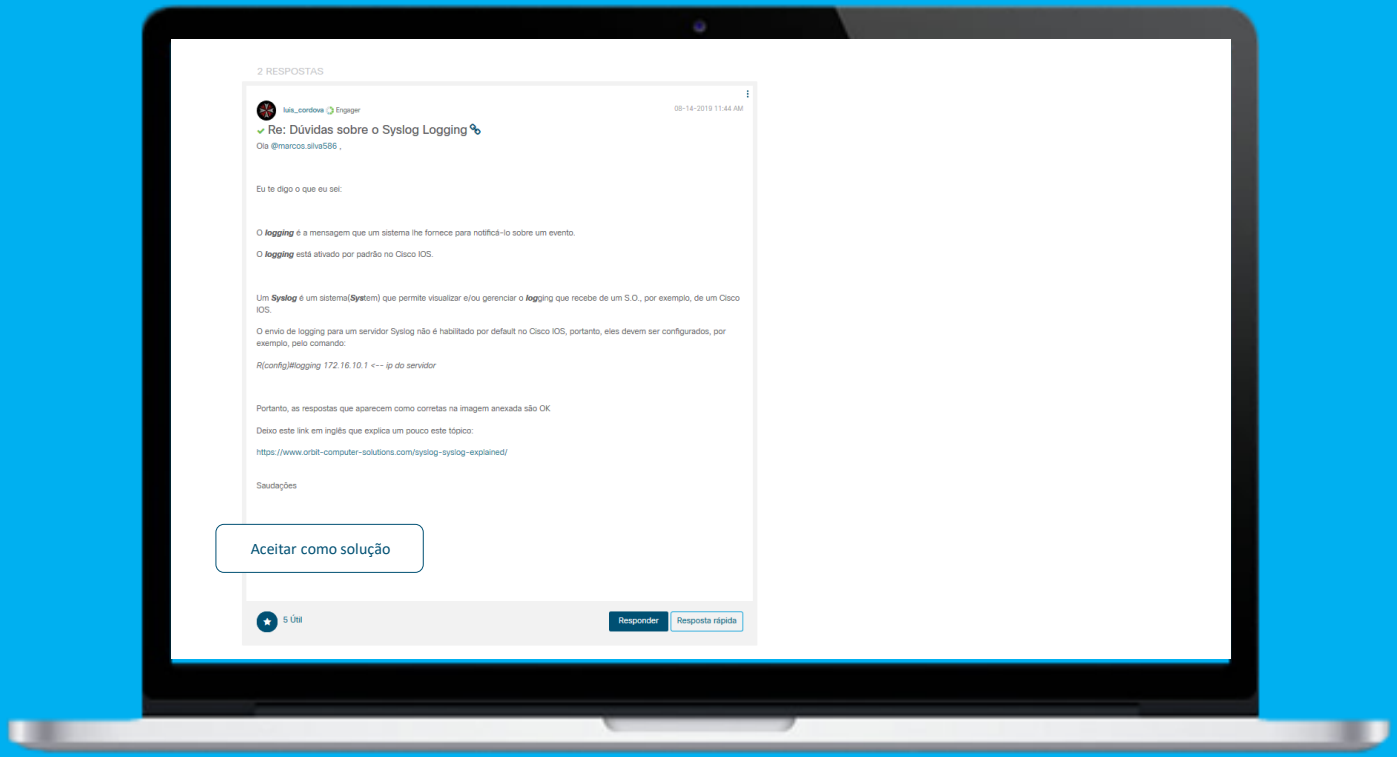
Mostre que a sua dúvida foi resolvida!

Embaixo de cada resposta se encontra o botão “Aceitar como solução”.

Se a resposta recebida resolve o seu problema, por favor faça como que todos saibam!

Simplesmente clique nesse botão:

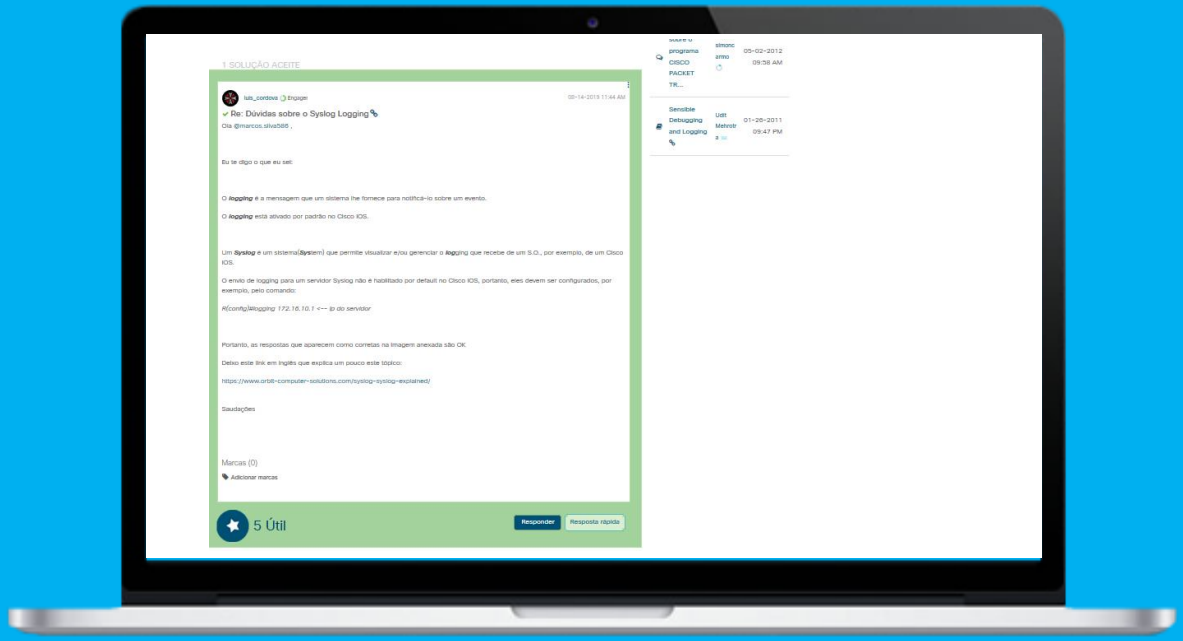
Aceitar como solução



Reconheça um problema solucionado!

Quando um membro que fez uma pergunta, considera que recebeu uma resposta satisfatória, ao clicar no botão “Aceitar como solução”.

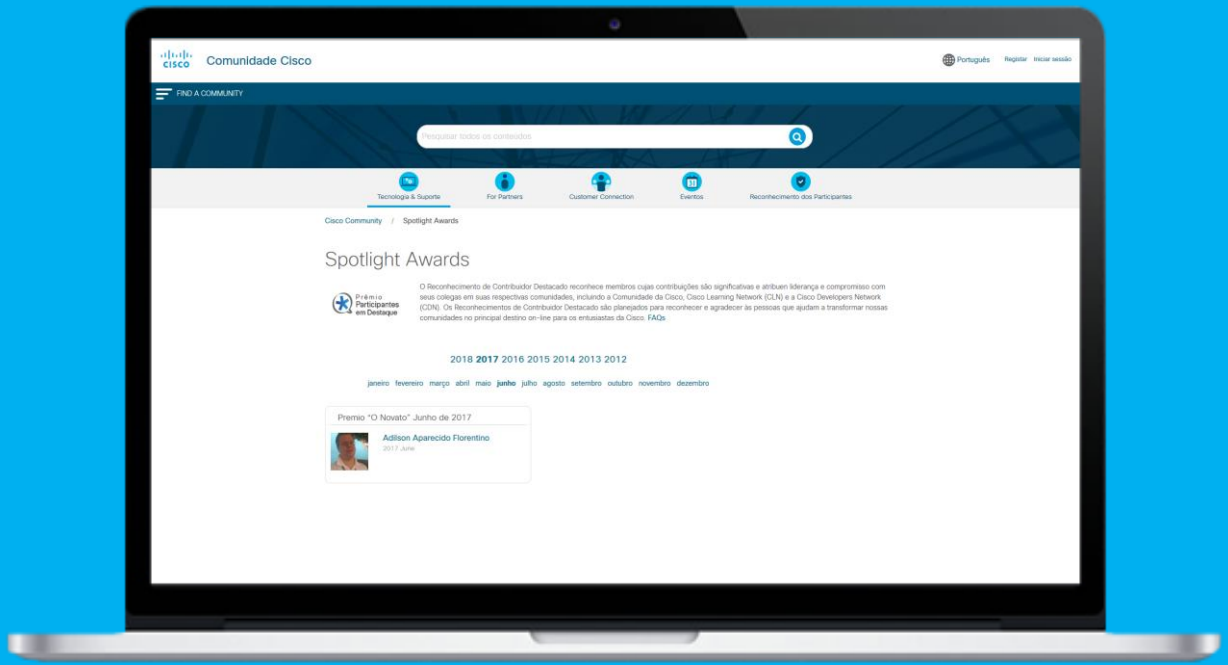
A resposta automaticamente fica envolvida de verde, e a pergunta recebe um retângulo como a palavra “Solucionado”.



Solucionado!

Seja um: “Contribuidor Destacado”!

Todas as pessoas que contribuem na Comunidade durante o mês, já seja respondendo perguntas, criando blogs, subindo documentos os videos. Correm o risco de serem reconhecidos pela Cisco como um contribuidor destacado!



Essa pessoa recebe um e-mail de notificação e um escudo distintivo no perfil e ao lado do nome de usuário dentro da Comunidade por 30 dias.

Assim, todos podem reconhecer quem é um “Contribuidor destacado” reconhecido pela Cisco.

Prêmio Participantes em Destaque

Veja a lista dos contribuidores destacados aqui: http://bit.ly/cdestacado

Especialista convidado

Luis Matos

Arquiteto de Soluções

Obrigado por unir-se a nós hoje!

Faça o download da apresentação nesse link:
https://community.cisco.com/t5/documentos-de-seguran%C3%A7a/webcast-slides-mitiga%C3%A7%C3%A3o-de-ataques-em-redes-de-computadores/ta-p/3918525

Publique as suas perguntas desde agora!

Use o painel de:
Perguntas & Respostas (Q&A) para enviá-las.

Essas, serão respondidas ao vivo no final da apresentação pelo especialista convidado.

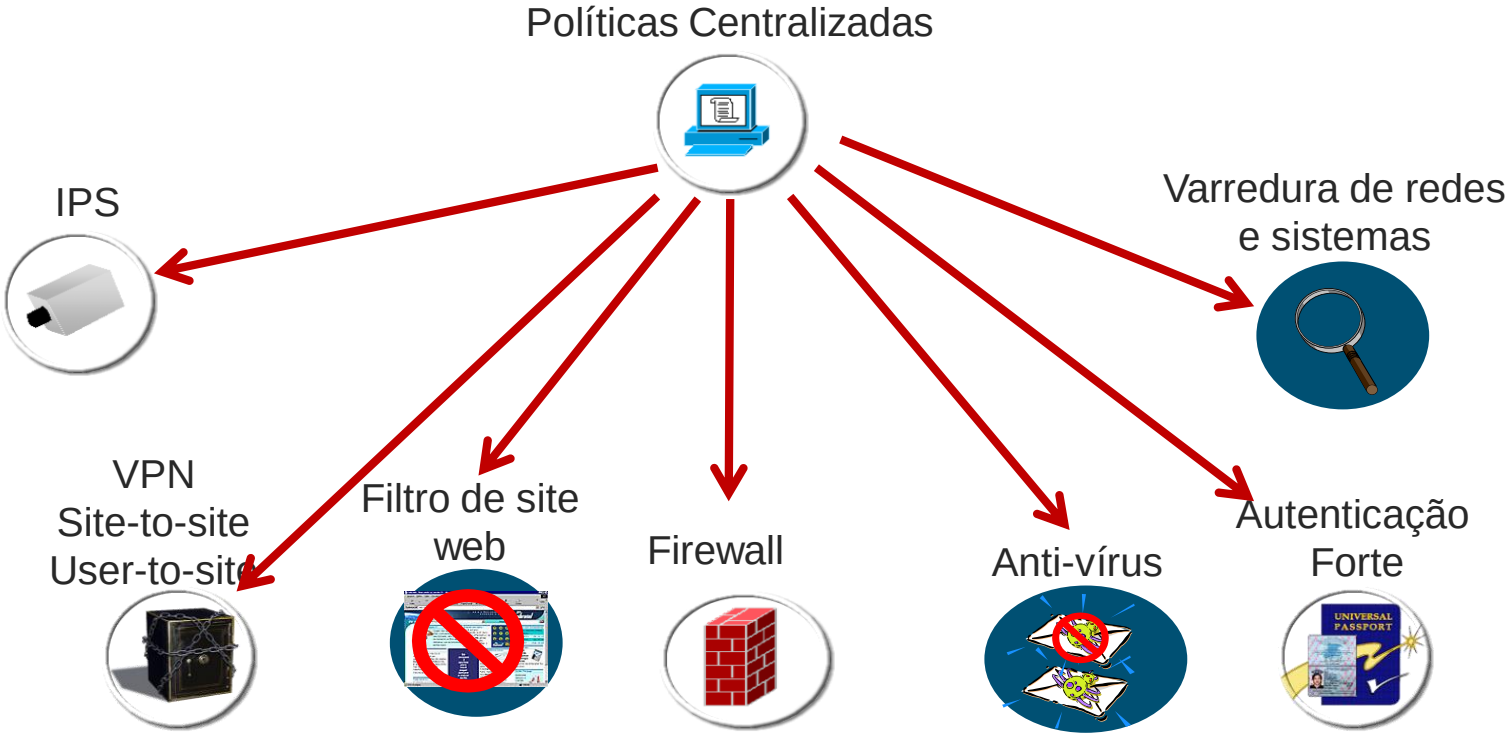
Agenda

- Introdução a segurança de redes
- Ataques na camada de acesso
- Controle de acesso utilizando 802.1x
- Cisco ISE como solução de controle de acesso
- Sizing de servidores e licenças
- Use cases para ambientes cabeado e wifi
- Melhores práticas para rollout
- Mitigação e visibilidade de Ransomware
- Criptografia na camada de acesso com MacSec
- Microsegmentação com TrustSec

Introdução

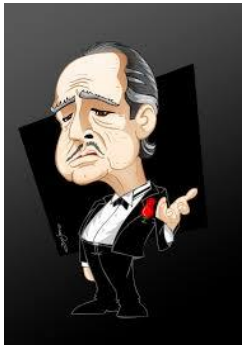
“O maior inimigo do conhecimento não é a ignorância; é a ilusão do conhecimento“ Stephen Hawking

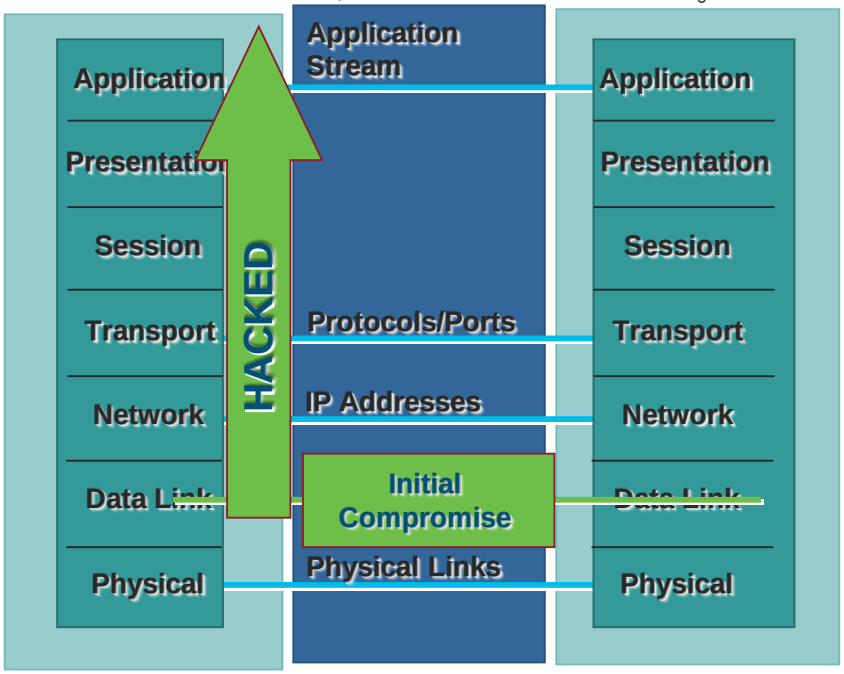
Dispositivos de Segurança



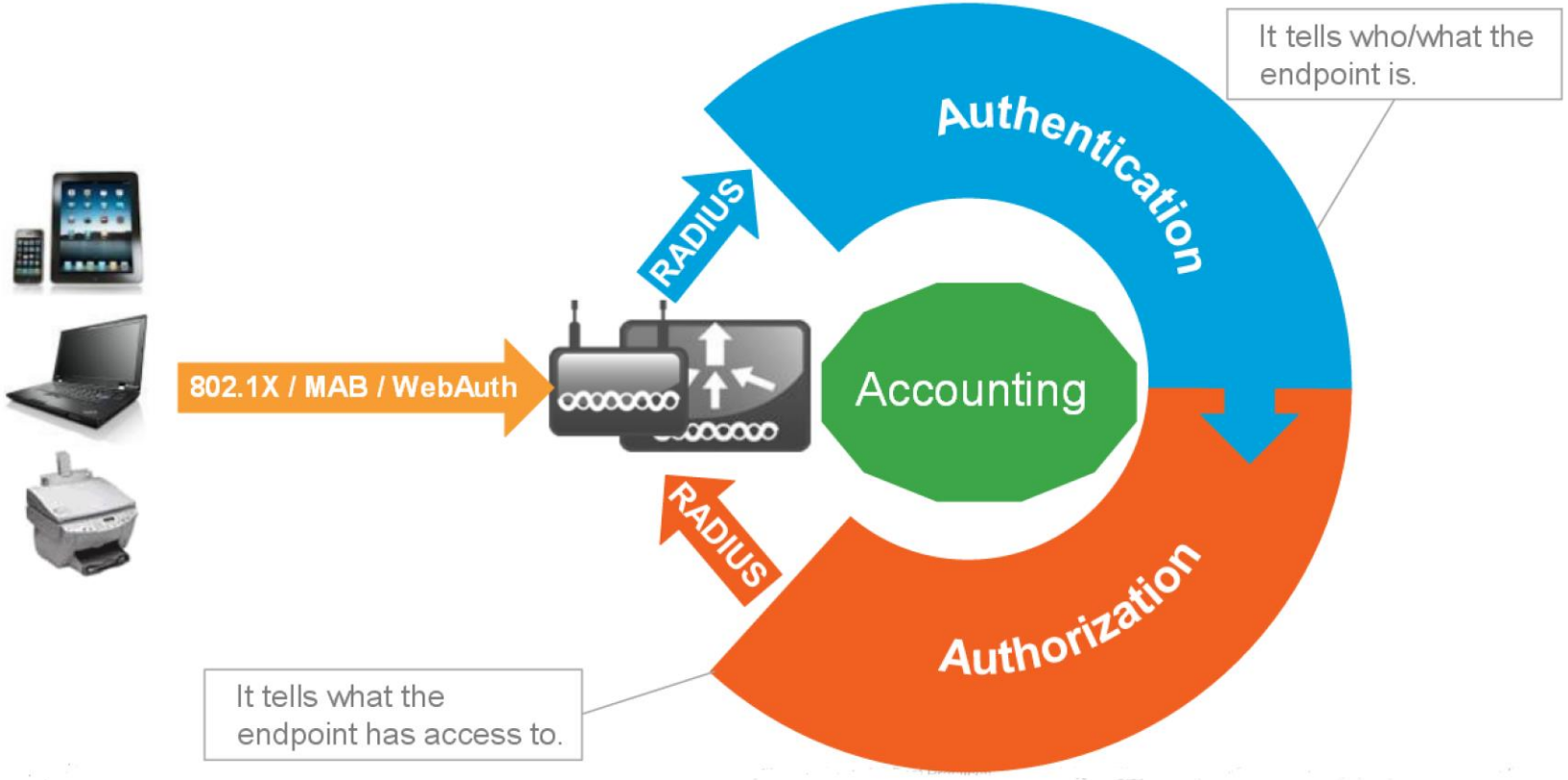
Exemplo de Ameaças – Camada de Acesso

- Efeito Dominó: A Camada com a implementação de segurança mais fraca compromete todas as demais.
- A Segurança é forte o tanto quanto o seu ponto mais vulnerável
- Na prática, podemos constatar que a camada de switches é a que recebe a menor atenção dos especialistas



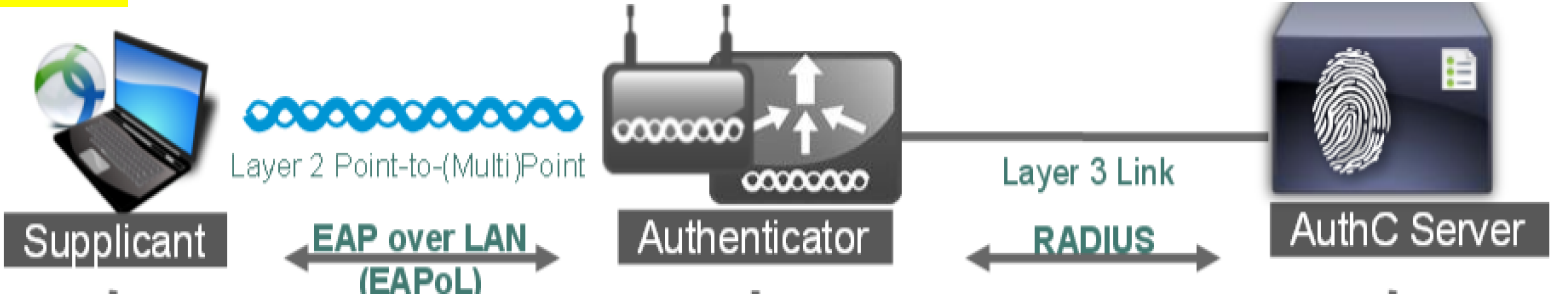


Projeto 802.1X – Frame Work



Projeto 802.1X – Tipos de Autenticação

EAP



MAB

Central Web Authentication

Profiling

Projeto 802.1X – Tipos de Autenticação

EAP Protocol support with ISE

EAP Protocol	ISE Internal	Windows AD	LDAP	RADIUS Token
EAP-MD5	Yes	No	No	No
EAP-TLS	No	Yes	Yes	No
PEAP MS-CHAPv2	Yes	Yes	No	No
PEAP EAP-TLS	No	Yes	Yes	No
EAP-FAST MS-CHAPv2	Yes	Yes	No	No
PEAP EAP-GTC	Yes	Yes	Yes	Yes
EAP-FAST EAP-GTC	Yes	Yes	Yes	Yes

Impressoras

Desktops, Telefone IP

Video Endpoints

Access Points

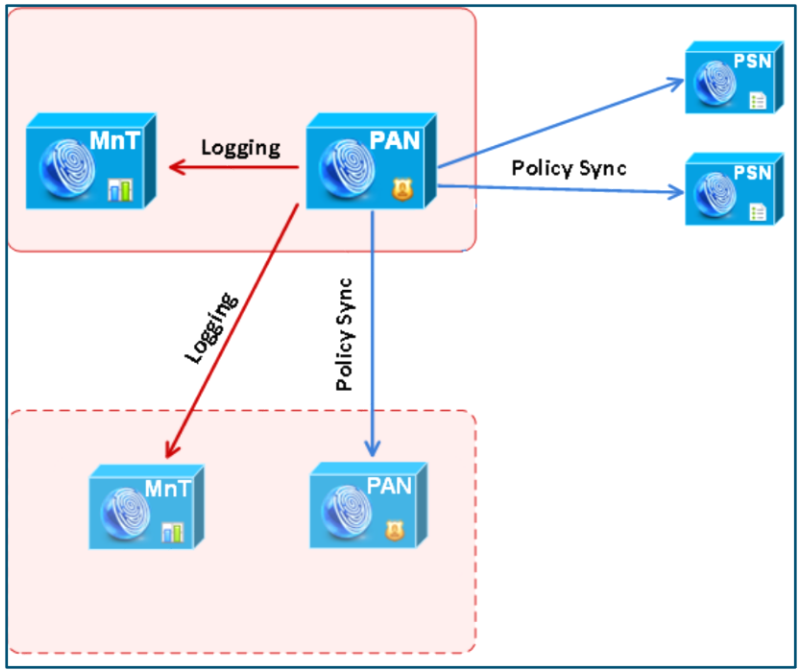
Projeto 802.1X – Base de Autenticacão

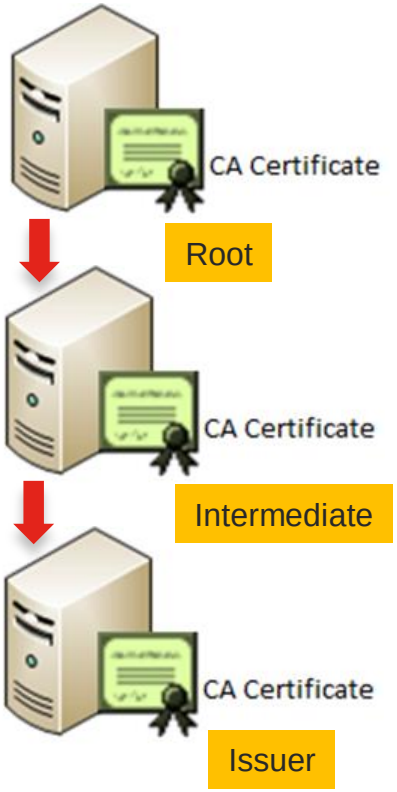
EAP Protocol	ISE Internal	Windows AD	LDAP	RADIUS Token
EAP-MD5	Yes	No	No	No
EAP-TLS	No	Yes	Yes	No
PEAP MS-CHAPv2	Yes	Yes	No	No
PEAP EAP-TLS	No	Yes	Yes	No
EAP-FAST MS-CHAPv2	Yes	Yes	No	No
PEAP EAP-GTC	Yes	Yes	Yes	Yes
EAP-FAST EAP-GTC	Yes	Yes	Yes	Yes

Projeto 802.1X – PKI

Sugestão

- PKI – Digital Certificates
  - All ISE nodes will use a valid digital certificate provided by customer's Internal CA (Microsoft 3 Layer PKI



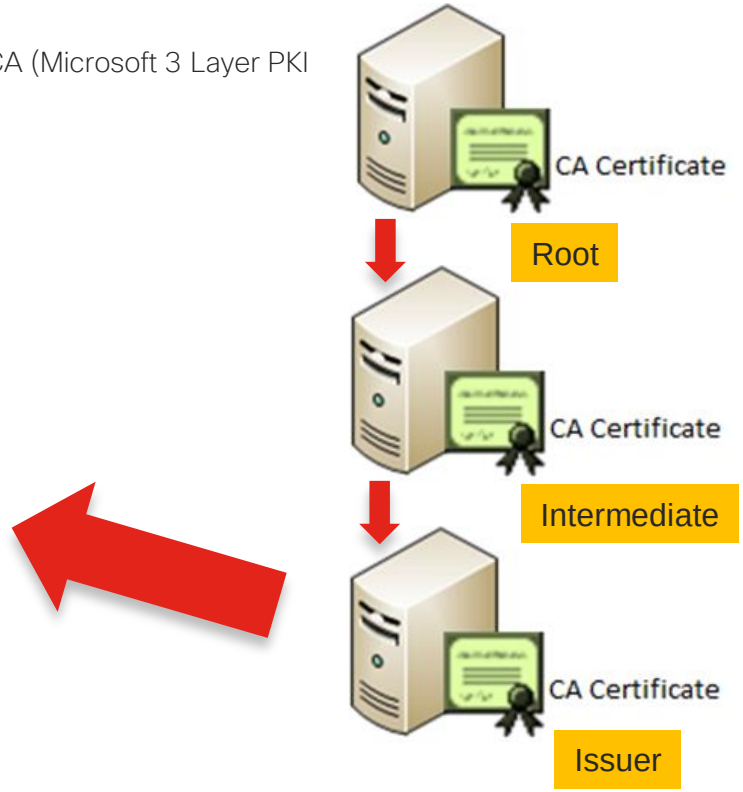


Projeto 802.1X – PKI

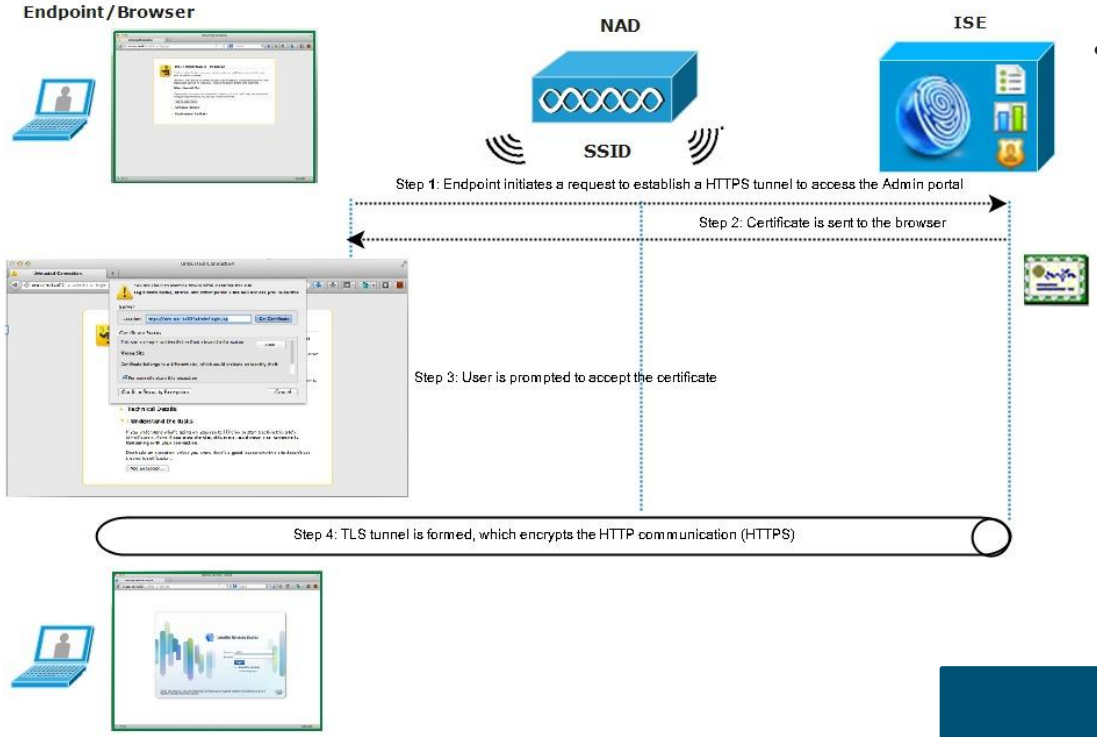
- PKI – Digital Certificates
  - All ISE nodes will use a valid digital certificate provided by customer's Internal CA (Microsoft 3 Layer PKI

- **Digital certificate considerations:**

1. The digital certificate must use X.509 v3
2. The digital certificate should use SHA-2
3. The digital certificate must contain the Client Authentication (OID "1.3.6.1.5.5.7.3.2") EKU
4. The digital certificate must be deployed for the Windows machines
5. The digital certificate must contain the machine account inside the "Subject Name"



Projeto 802.1X – PKI



- Trusted Certificates
  - Devices must trust C.A. certificate
  - Used for ISE CUBE deployment
  - MIC or LSC for Cisco IP Phones

Projeto 802.1X – Microsoft Active Directory (Sites)

Join Operations	Leave Operations	Cisco ISE Machine Accounts
For the account that is used to perform the join operation, the following permissions are required: ▪ Search Active Directory (to see if a Cisco ISE machine account already exists) ▪ Create Cisco ISE machine account to domain (if the machine account does not already exist) ▪ Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname) It is not mandatory to be a domain administrator to perform a join operation.	For the account that is used to perform the leave operation, the following permissions are required: ▪ Search Active Directory (to see if a Cisco ISE machine account already exists) ▪ Remove Cisco ISE machine account from domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required: ▪ Ability to change own password ▪ Read the user/machine objects corresponding to users/machines being authenticated ▪ Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) ▪ Ability to read tokenGroups attribute You can precreate the machine account in Active Directory, and if the SAM name matches the Cisco ISE appliance hostname, it should be located during the join operation and re-used. If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join.

Protocol	Port (remote-local)	Target	Authenticated	Notes
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	No	–
MSRPC	445	Domain Controllers	Yes	–
Kerberos (TCP/UDP)	88	Domain Controllers	Yes (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	Yes	–
LDAP (GC)	3268	Global Catalog Servers	Yes	–
NTP	123	NTP Servers/Domain Controllers	No	–
IPC	80	Other ISE Nodes in the Deployment	Yes (Using RBAC credentials)	–

Pergunta 1

- Qual node é responsável pela autenticação do dispositivo?

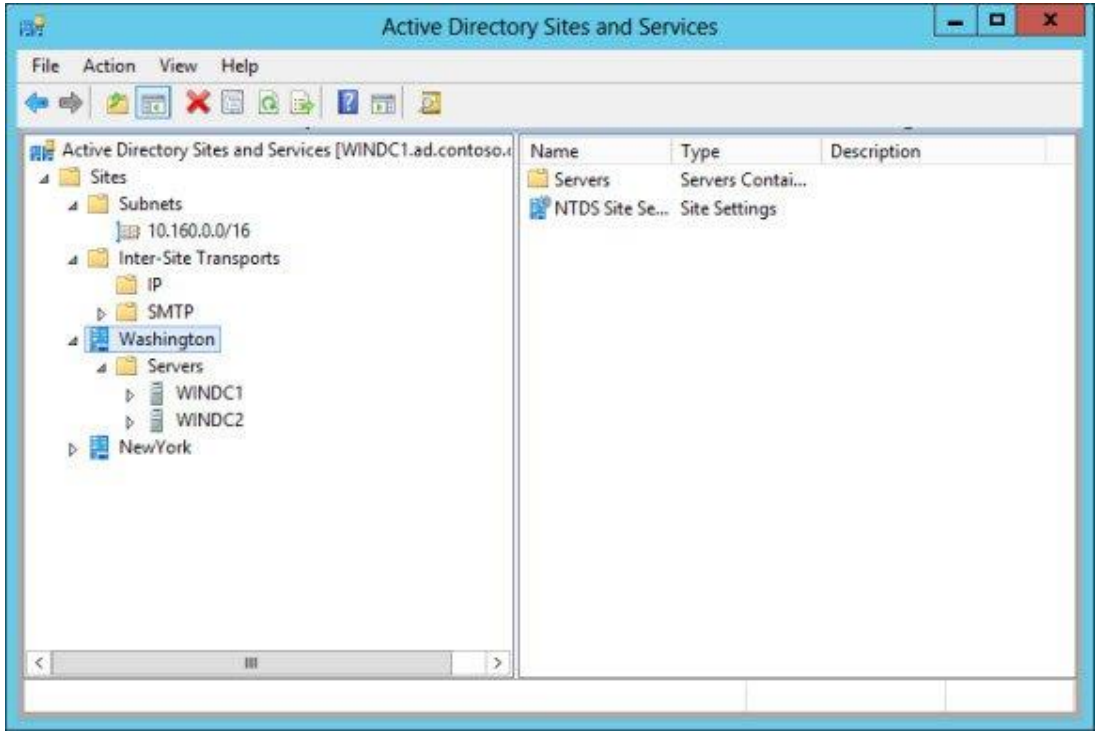
A. PAN

B. MNT

C. PSN

Projeto 802.1X – Microsoft Active Directory (Sites)

- Servidores DC dedicados
  - Para este projeto, existem servidores DC dedicados



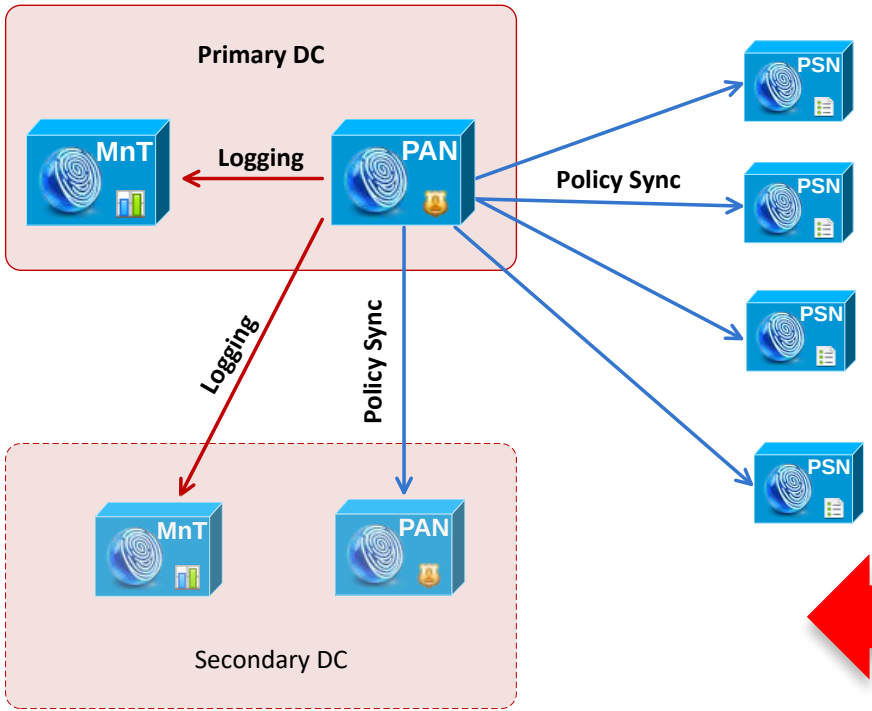
Projeto 802.1X – Microsoft DNS

DNS Server

While configuring your DNS server, make sure that you take care of the following:

- All DNS servers configured in Cisco ISE must be able to resolve all forward and reverse DNS queries for all domains you wish to use.
- All DNS server must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.
- We recommend that you add the server IP addresses to SRV responses to improve performance.
- Avoid using DNS serversthat query the public Internet. They can cause delays and leak information about your network when an unknown name has to be resolved

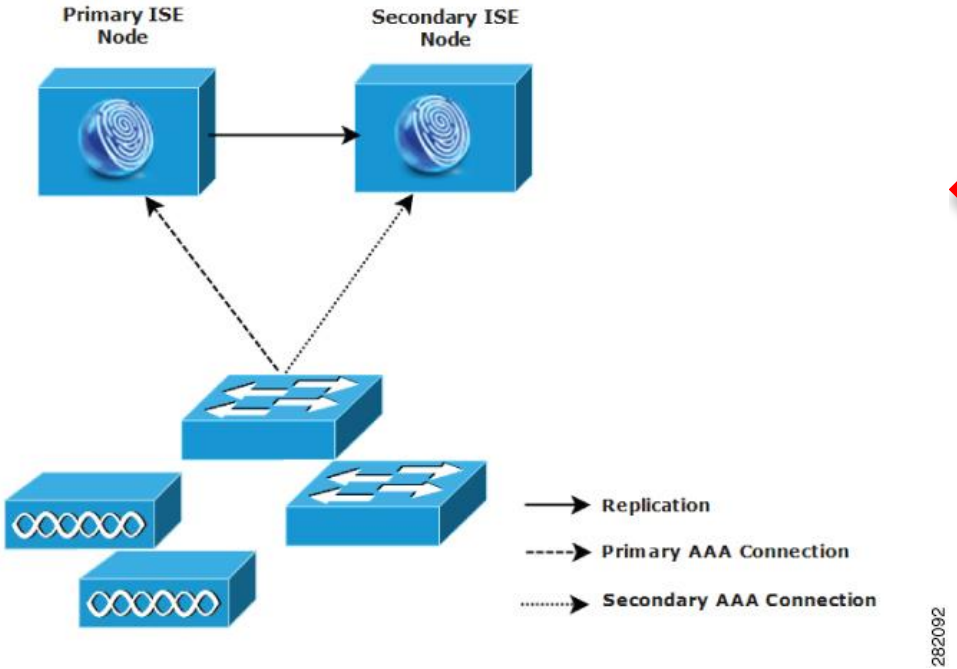
Projeto 802.1X – Identity and Access Control Design



- ISE PAN and MnT Servers
  - Only one PAN instance can be defined as the primary PAN, which will be placed in the Secondary Data Center for the customer deployment
  - All configuration changes that are made on the Primary PAN server will be synced to all nodes within the ISE deployment

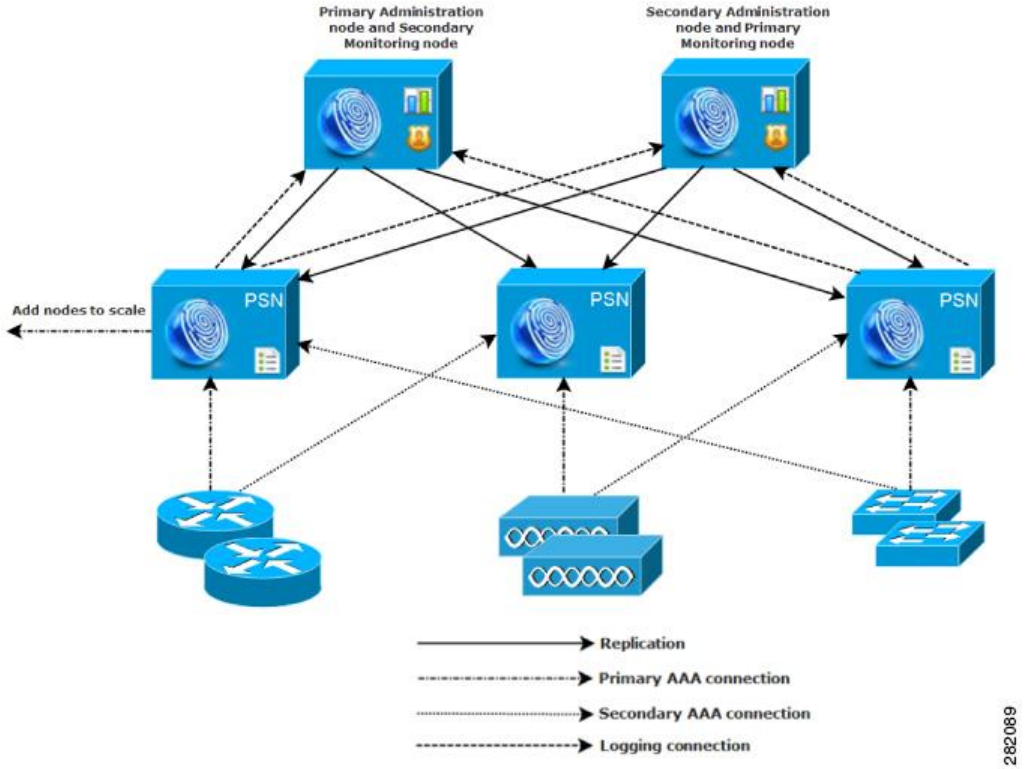
Large Deployment

Projeto 802.1X – Identity and Access Control Design



Small Deployment

Projeto 802.1X – Identity and Access Control Design



Medium Deployment

Projeto 802.1X – Identity and Access Control Design

Attribute	ISE 2.2 Maximums	ISE 2.4 Maximums	ISE 2.6 Maximums
Maximum number of concurrent sessions in a Dedicated deployment (Separate PAN, MnT, and PSN nodes)	250,000 for 3495 as PAN and 3495 as MnT 500,000 for 3595 as PAN and 3595 as MnT	34xx not supported 500,000 for 3595 as PAN and 3595 as MnT	2,000,000 - 3695 as PAN and MnT 500,000 -3595 as PAN and MnT
Maximum number of concurrent sessions in a Hybrid deployment (PAN & MnT on a single node and dedicated PSNs)	5,000 for 3415 as PAN+MnT 10,000 for 3495 as PAN+MnT 7,500 for 3515 as PAN+MnT 20,000 for 3595 as PAN+MnT	34xx not supported 7,500 for 3515 as PAN+MnT 20,000 for 3595 as PAN+MnT	10,000 for 3615 as PAN+MnT 25,000 for 3655 as PAN+MnT 50,000 for 3695 as PAN+MnT 7500 for 3515 as PAN+MnT 20,000 for 3595 as PAN+MnT
Maximum number of concurrent sessions in a Standalone deployment (PAN, MnT, and PSN personas all on a single node)	5,000 for 3415 10,000 for 3495 7,500 for 3515 20,000 for 3595	34xx not supported 7,500 for 3515 20,000 for 3595	10,000 for 3615 25,000 for 3655 50,000 for 3695 7500 for 3515 20,000 for 3595
Maximum number of PSNs in a Dedicated deployment (Separate PAN, MnT and PSN nodes)	40 for 3495 as PAN	50 for 3595 as PAN	50 for 3595 as PAN 50 for 3695 as PAN

LARGE

LARGE

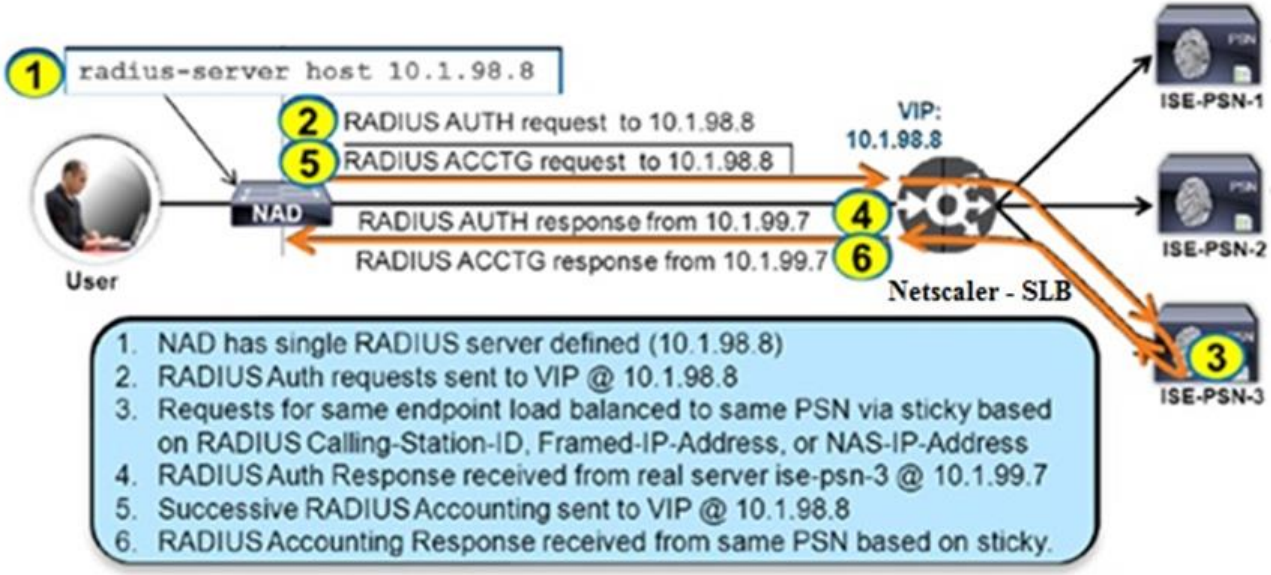
Projeto 802.1X – Identity and Access Control Design

	3415	3495	3515	3595	3615	3655	3695
ISE Version	ISE 2.0 / 2.1+	ISE 2.0 / 2.1+	ISE 2.0.1 / 2.1+	ISE 2.0.1 / 2.1+	ISE 2.6	ISE 2.6	ISE 2.6
Maximum Concurrent Sessions	5,000	20,000	5,000 / 7,500	20,000 / 40,000	10,000*/10,000	25000*/50,000	50,000*/100,000

* concurrent sessions for hybrid deployment

Projeto 802.1X – Load Balance

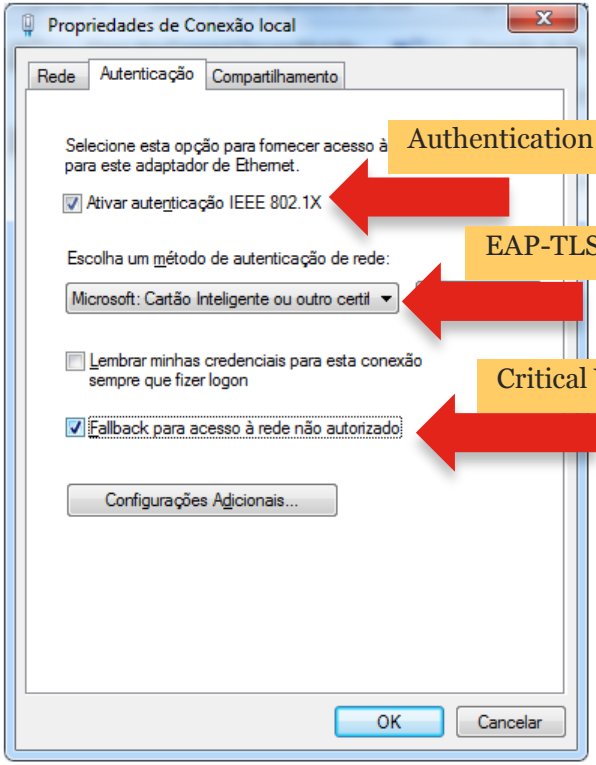
- Radius Load Balance



Projeto 802.1X – Identity and Access Control Design

- ISE Topology
  - Quantidade: 4 Virtual IP no Load Balancer, nos dois datacenters:
    - 1 VIP in em DC-1 para Radius (udp: 1812/1813)
    - 1 VIP in em DC-1 para Postura (tcp: 8443/8905)
    - 1 VIP in em DC-2 para Radius (udp: 1812/1813)
    - 1 VIP in em DC-2para Postura (tcp: 8443/8905)

    ** Verificar se o balanceador teria um melhor comportamento utilizando uma mesma VIP para Radius e Postura.
  - Requerimentos
    - Presistência de conexao (sticky connection) = 8 horas, utilizando o atributo radius 31 (Calling-Station-Id), onde dispositivo deve sempre utilizar o mesmo real server para Radius e Postura.
    - Probe = Radius probe , utilizando usuário do Active Directory
  - NAT
    - Quando um PSN iniciar comunicacao com um endpoint, oriundo de um processo de CoA (udp: 1700/3799) ou SNMP (udp: 161/162), deverá ser realizado NAT do IP de origem do PSN para o IP da VIP do loadbalancer.
  - Load Sharing
    - 50% dos sites devem utilizar a VIP do DC-1 como Radius primário e a VIP do DTC como radius secundário
    - 50% dos sites devem utilizar a VIP do DC-2como Radius primário e a VIP do CTC como radius secundário



Authentication Enable

EAP-TLS

Critical VLAN

Configuração Automática com Fio	O Serviço de Configuração Automática de Rede com Fio (DOT3SVC) é responsável pela aut...
Configuração Automática de WLAN	O serviço WLANSVC fornece a lógica necessária para configurar, descobrir, se conectar e de...
Configuração Automática de WWAN	Esse serviço gerencia placas de dados/adaptadores de módulo inseridos de banda larga mó...
Configuração da Área de Trabalho Remota	O serviço RDCS (serviço de Configuração da Área de Trabalho Remota) é responsável por t...
Construtor de Pontos de Extremidade de Áudio d...	Gerencia dispositivos de áudio para o serviço Áudio do Windows. Se esse serviço for interro...
Coordenador de transações distribuídas	Coordena as transações que incluem vários gerenciadores de recursos, como bancos de da...

Projeto 802.1X – Use Cases

- Wired Access (Dot1X)
  - Corporate Computers
    - Authentication = EAP-TLS using corporate PKI digital certificate (Computer Certificate)
    - Authorization = Computer must belongs to a specific Active Directory group (domain\Domain Computers)
    - Results = The switch will receive **Data** Domain Permission
  - IP Phones
    - Authentication = EAP-TLS using a digital certificate provided by Cisco factory (MIC) or CALL MANAGER (LSC)
    - Authorization = Username must starts with to a specific string (CP or SEP)
    - Results = The switch will receive **Voice** Domain Permission

    Note: Cisco will test the IP Phone authentication using the equipment model that is going to be used for the corporate environment
  - Access Points
    - Authentication = EAP-FAST using single username and password locate inside ISE internal database
    - Authorization = Device must belongs to a specific device-group (ACCESS-POINTS)
    - Results = The switch will receive **Data** Domain Permission

Projeto 802.1X – Use Cases

- Wired Access (MAB)
  - Corporate Printers
    - Authentication = MAB , MAC Address locate inside ISE internal database
    - Authorization = Device must belongs to a specific device-group (for instance: ISE-PRINTERS) which will be registered on respective MyDevices Portal page.
    - Results = The switch will receive Data Domain Permission ; ISE will restrict traffic using DACL (traffic will be allowed only to the print server)
  - PXE re-image procedure
    - Authentication = MAB , MAC Address locate inside ISE internal database (using a WEB Portal)
    - Authorization = Device must belongs to a specific device-group (for instance: ISE-Altiris)
    - Results = The switch will execute a smart-port macro ADMIN_ALTIRIS; ISE will restrict traffic using DACL (traffic will be allowed only to the Altiris servers)

ISE – Use Cases

- Wireless Access (Dot1X)
  - SSID: CORPORATE (Corporate Computers)
    - Authentication = EAP-TLS using corporate PKI digital certificate (Computer Certificate)
    - Authorization = Computer must belongs to a specific Active Directory group (for instance: domain\Domain Computers)

      SSID must be equals to ?? (ADMIN)
    - Results = ISE will instruct WLC to allow the traffic (Internal LAN Access)
  - SSID: BYOD (Corporate Smartphones)
    - Authentication = EAP-TLS using corporate PKI digital certificate (User Certificate)
    - Authorization = Users must belongs to a specific Active Directory group (for instance: domain\Domain Users)

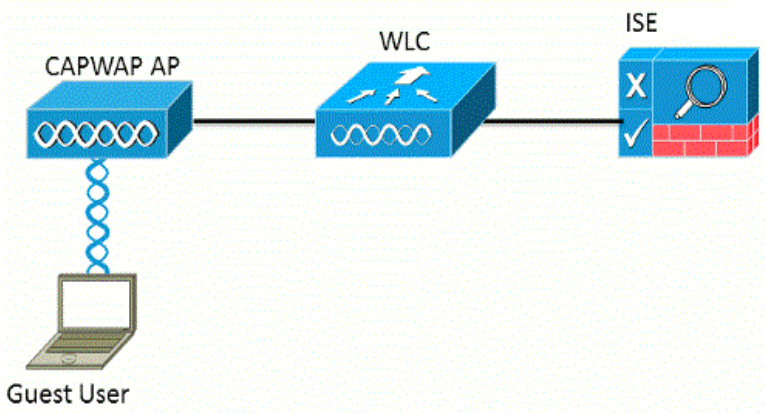
      SSID must be equals to ?? (ADMIN)
    - Results = ISE will instruct WLC to allow the traffic (Internet Access Only)

ISE – Use Cases

- Wireless Access (Dot1X)
  - SSID: GUESTS
    - Authentication = CWA , using user's generated at OBS Sponsor page
    - Authorization = Users must belongs to a specific group created on sponsor page (For instance: ISE-Guests)

      SSID must be equals to ?? (Guests)
    - Results = ISE will instruct WLC to allow the traffic (Internet Access Only)

ISE – Use Cases



- CWA (Central WEB Authentication)
  - The user associates to the web authentication Service Set Identifier (SSID)
  - The user opens the browser.
  - The WLC redirects to the guest portal as soon as a URL is entered.
  - The user authenticates on the portal.
  - The guest portal redirects back to the WLC with the credentials entered.
  - The WLC authenticates the guest user via RADIUS.
  - The WLC redirects back to the original URL.
  - This flow includes several redirections. The new approach is to use CWA. This method works with ISE (versions later than 1.1) and WLC (versions later than 7.2). The flow includes these steps:
  - The user associates to the web authentication SSID, which is in fact open+macfiltering and no layer 3 security.
  - The user opens the browser.
  - The WLC redirects to the guest portal.
  - The user authenticates on the portal.

ISE – Use Cases (CWA & IDM Integration)

Sign On (Wireless IPANEMA - Press & Broadcast Users)

Welcome to the **Rio 2016 Olympic Games** !

New WiFi user? Forgot password?

Username:

Password:

Please read the terms and conditions.

I agree to the terms and conditions

Sign On

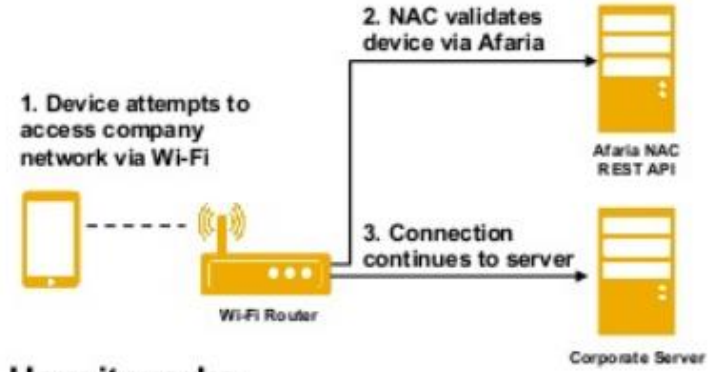
ISE – Use Cases (MDM Integration)

Un-configured APP

Confused User

Fully Configured APP

Happy User



How it works

(1) User attempts to connect to corporate Wi-Fi

(2) NAC queries Afaria via REST API to validate device is known and secure

If yes, (3) NAC allows connection

If no, NAC re-directs user to a web page that describes how to make device compliant and links to the Afaria Self Service portal

Not safe for the enterprise

Lacking enterprise controls

- No security
- No app management
- No enterprise app portal
- No certificates

Safe for the enterprise

Enterprise control

- Power-on-password
- Enterprise App Portal fully configured
- Certificates for SSO, Wi-Fi, VPN, and Email deployed
- Apps enabled for configuration
- Policies are automatically deployed

Projeto 802.1X – Fall Back

Critical Auth for Data and Voice

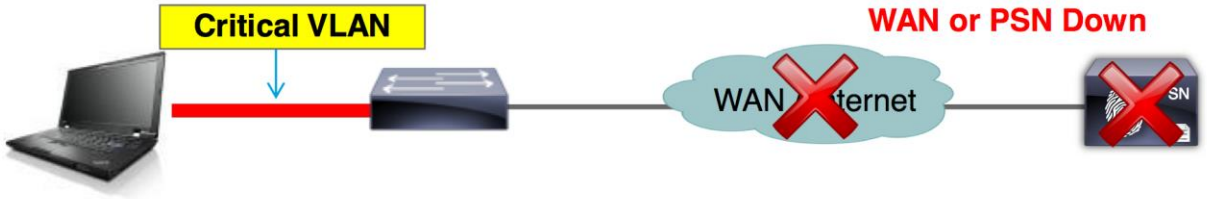

```
interface fastEthernet 3/48
 dot1x pae authenticator
 authentication port-control auto
 authentication event server dead action authorize vlan x
 authentication event server dead action authorize voice
```

```
# show authentication sessions interface fa3/48
...
Critical Authorization is in effect for domain(s) DATA and VOICE
```

Projeto 802.1X – Fall Back

Inaccessible Authentication Bypass (IAB)

Also Known As “Critical Auth VLAN” for Data

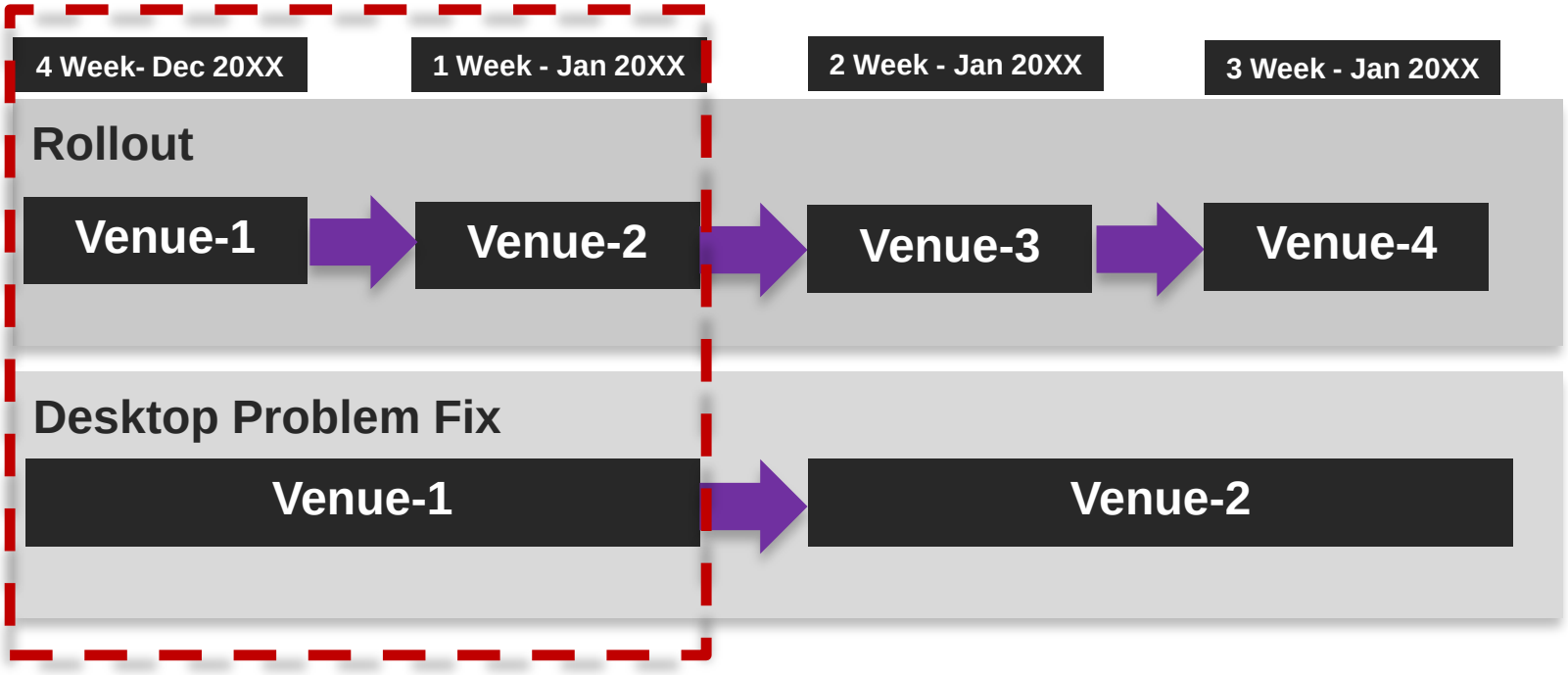


- Switch detects PSN unavailable by one of two methods
  - Periodic probe
  - Failure to respond to AAA request
- Enables port in critical VLAN
- Existing sessions retain authorization status
- Recovery action can re-initialize port when AAA returns

Critical VLAN can be anything:
- Same as default access VLAN
- Same as guest/auth-fail VLAN
- New VLAN

```
authentication event server dead action authorize vlan 100
authentication event server alive action reinitialize
```

Projeto 802.1X – Deployment



The rollout waves should not following the desktop problem fix waves, they should be totally independent activities, because it will cause a huge delay in the Project implantation time line.

Pergunta 2

- Qual método de authenticação é vulnerável a spoofing?

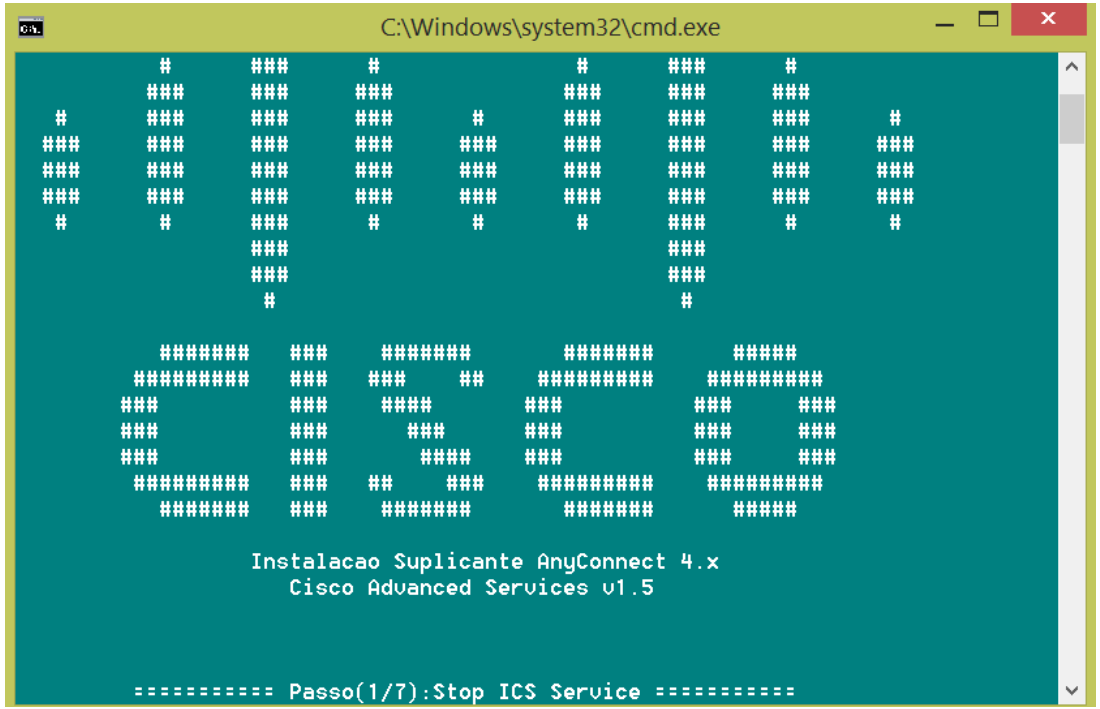
A. MAB

B. EAP-PEAP

C. EAP-TLS

Projeto 802.1X – Supplicant Deployment

1) Use a script to deploy Anyconnect Modules and XML files



The script will be used from a network drive or USB drive, just a double click is needed to prepare all the desktop environment (modules and xml's)

ISE Rollout – Supplicant Deployment

1) Use a script to deploy Anyconnect Modules and XML files

Script Steps

Step-1: Stop ICS Service (or other non compatible software, if it is running)

Step-2: Increase Maximum Registry Interfaces (if needed)

Step-3: Install Pre-Deployment Module

Step-4: Install NAM Module

Step-5: Install Posture Module

Step-6: Copy XML Files

Step-7: Modify Registry Multi User Support (if needed)

Step-8: Reboot

2:15 Minutes To complete all

AnyConnect Script

ISE Rollout – Supplicant Deployment

Sugestão

1) Use a Deployment Solution to launch Anyconnect Modules and XML files

Script Steps

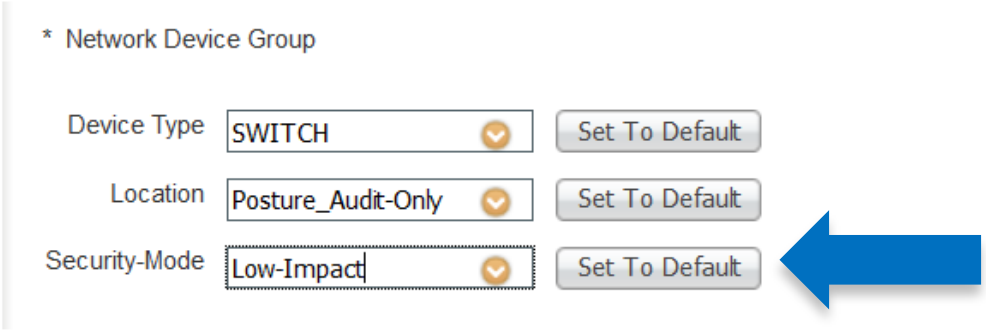
```
REM *** PACOTES ***

msiexec /package anyconnect-win-4.6.03049-core-vpn-predeploy-k9.msi /quiet /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1
msiexec /package anyconnect-win-4.6.03049-nam-predeploy-k9.msi /quiet /norestart /passive
msiexec /package anyconnect-win-4.6.03049-iseposture-predeploy-k9.msi /quiet /norestart /passive
REM *** ARQUIVOS A SEREM COPIADOS ***
copy configuration.xml "%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\"
>NUL
copy ISEPostureCFG.xml "%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\" >NUL
```

- /quiet - there is no user interaction
- /passive - unattended mode, the installation shows only a progress bar
- /norestart – no reboot required· PRE_DEPLOY_DISABLE_VPN=1 disable VPN client

OBS: O diretório "%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\" deve ser criadas antes de copiar o arquivo ISEPostureCFG.xml

ISE Rollout – Low Impact Mode

2) Use Enhanced Low Impact Mode (Dot1x & Posture – Per Switch Basis)



Security-Mode = Low_Impact : This option will use the closed mode Police Set but it will allow the devices which are not able to connect the network using dot1x (in case of a supplicant and/or digital certificate misconfiguration) to access the network using MAB.

Importante Information: The switch is not configured in open mode, instead, it is configures in closed mode.

ISE Rollout – Low Impact Mode

3) Use Enhanced Low Impact Mode (Dot1x & Posture – Per Switch Basis)

☑	GUESTS	if	AD-Win2012:ExternalGroups EQUALS cisco.com/Users/BRA-GUESTS	then	PERMIT_BRA-GUESTS AND BRA_SG_GUETS
☑	BYOD	if	AD-Win2012:ExternalGroups EQUALS cisco.com/Users/BRA-BYOD	then	PERMIT_BRA-BYOD AND BRA_SG_BYOD
☑	USERS	if	AD-Win2012:ExternalGroups EQUALS cisco.com/Users/Domain Users	then	PERMIT_BRA-USERS AND BRA_SG_USERS
☑	LOW IMPACT MODE	if	DEVICE:Security-Mode EQUALS Security-Mode#Low-Impact	then	PROBLEM-DOT1X
☑	Default	if no matches, then	DenyAccess		

Security-Mode = Low_Impact : The authorization police will be used in a "per switch basis fashion". There is no need of a new police set, it will use the closed mode one.

ISE Rollout – Low Impact Mode

4) Use Enhanced Low Impact Mode (Dot1x & Posture – Per Switch Basis)

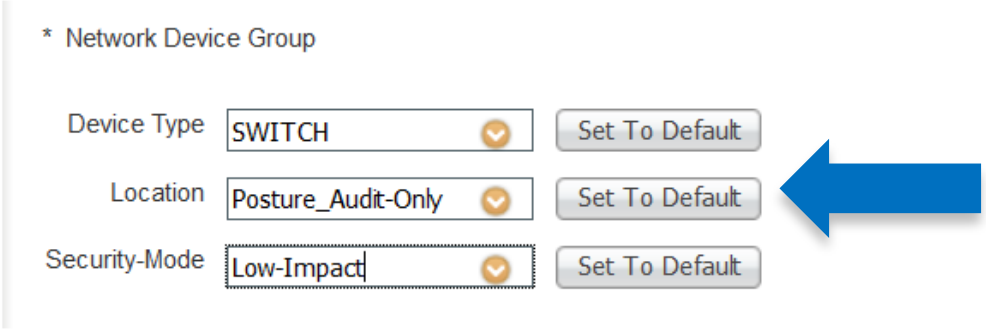
802.1x ISE - Low Impact Mode (30/09/2016)					
Data Devices (Total = 22, Sem certificado e/ou Suplicante não configurado)					
Interface	**MAC Address**	**Method**	**Domain**	**IP Address**	**OUI**
Fa9/32	641c.676e.ecf6	mab	DATA	10.14.132.17	DIGIBRAS INDUSTRIA DO BRASILS/A
Gi1/29	7071.bc07.bd01	mab	DATA	10.14.132.31	PEGATRON CORPORATION
Fa8/22	009c.0202.7cb2	mab	DATA	10.14.132.119	HEWLETT PACKARD
Gi3/5	3464.a9d5.9bac	mab	DATA	10.14.132.12	HEWLETT PACKARD
Gi2/25	641c.677b.2521	mab	DATA	10.14.132.129	DIGIBRAS INDUSTRIA DO BRASILS/A
Gi2/21	641c.677f.955c	mab	DATA	10.14.132.24	DIGIBRAS INDUSTRIA DO BRASILS/A
Gi2/8	000c.2989.de7b	mab	DATA	10.14.132.143	VMWARE, INC.
Fa8/41	0006.2400.a8ba	mab	DATA	10.14.132.23	GENTNER COMMUNICATIONS CORP.
Gi1/18	0000.0000.0001	mab	DATA	10.14.132.112	XEROX CORPORATION
Fa9/12	641c.675f.d12a	mab	DATA	10.14.132.65	DIGIBRAS INDUSTRIA DO BRASILS/A
Fa10/47	000b.001e.f067	mab	DATA	10.14.132.61	FUJIAN START COMPUTER EQUIPMENT CO.,LTD
Fa10/44	082e.5fbd.67a1	mab	DATA	10.14.132.53	HEWLETT PACKARD
Gi2/30	5cf9.dded.9e26	mab	DATA	10.14.132.138	DELL INC.
Gi2/7	902b.34f6.229e	mab	DATA	Unknown	GIGA-BYTE TECHNOLOGY CO.,LTD.
Gi1/34	74e6.e2d1.591e	mab	DATA	10.14.132.99	DELL INC.
Gi1/30	902b.34f4.ee9f	mab	DATA	Unknown	GIGA-BYTE TECHNOLOGY CO.,LTD.
Fa8/3	406c.8f33.2ea6	mab	DATA	Unknown	APPLE, INC.
Gi2/19	a820.6644.2d58	mab	DATA	10.14.132.63	APPLE, INC.
Gi1/21	902b.34f6.2476	mab	DATA	192.168.0.10	GIGA-BYTE TECHNOLOGY CO.,LTD.
Gi2/5	641c.6768.6e8a	mab	DATA	Unknown	DIGIBRAS INDUSTRIA DO BRASILS/A
Gi1/48	1098.36ff.429a	mab	DATA	10.14.132.11	DELL INC.

Using this method we can easily find the **misconfigured devices** executing the command "show authentication sessions | i mab" .

With this report the field support team could solve the desktop issues quickly.

ISE Rollout – Low Impact Mode

5) Use Enhanced Low Impact Mode (Dot1x & Posture – Per Switch Basis)



Location = Posture_Audit-Only : This option will use the closed mode Police Set but it will allow the devices which are not posture compliant (in case of a antivirus and/or registry key misconfiguration) to access the network without any restriction (as a compliant machine).

ISE Rollout – Low Impact Mode

6) Use Enhanced Low Impact Mode (Dot1x & Posture – Per Switch Basis)

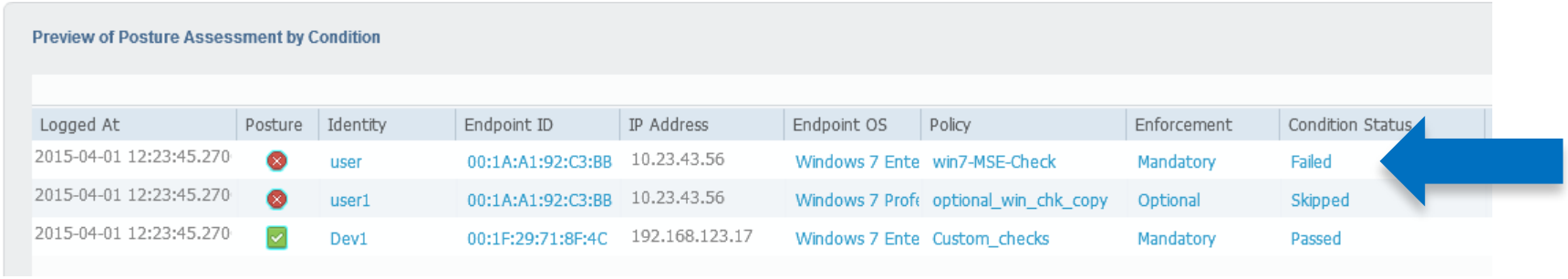
Status	Rule Name		Identity Groups		Operating Systems	Other Conditions
✓	Antivirus - Closed Mode	If	Any	and		DEVICE:Location NOT_EQUALS All Locations#Posture_Audit-Only
✓	Antivirus - Low Impact	If	Any	and		DEVICE:Location EQUALS All Locations#Posture_Audit-Only

Antivirus – Closed Mode : This posture will be executed only for desktops connected to switches in closed mode. These desktops will only have access to the network in case of a **compliant status**.

Antivirus – Low Impact: This posture will be executed only for desktops connected to switches in low impact mode. These desktops will have access to the network even if they are in a **not compliant status**.

ISE Rollout – Low Impact Mode

7) Use ISE reports to identify the non compliant devices

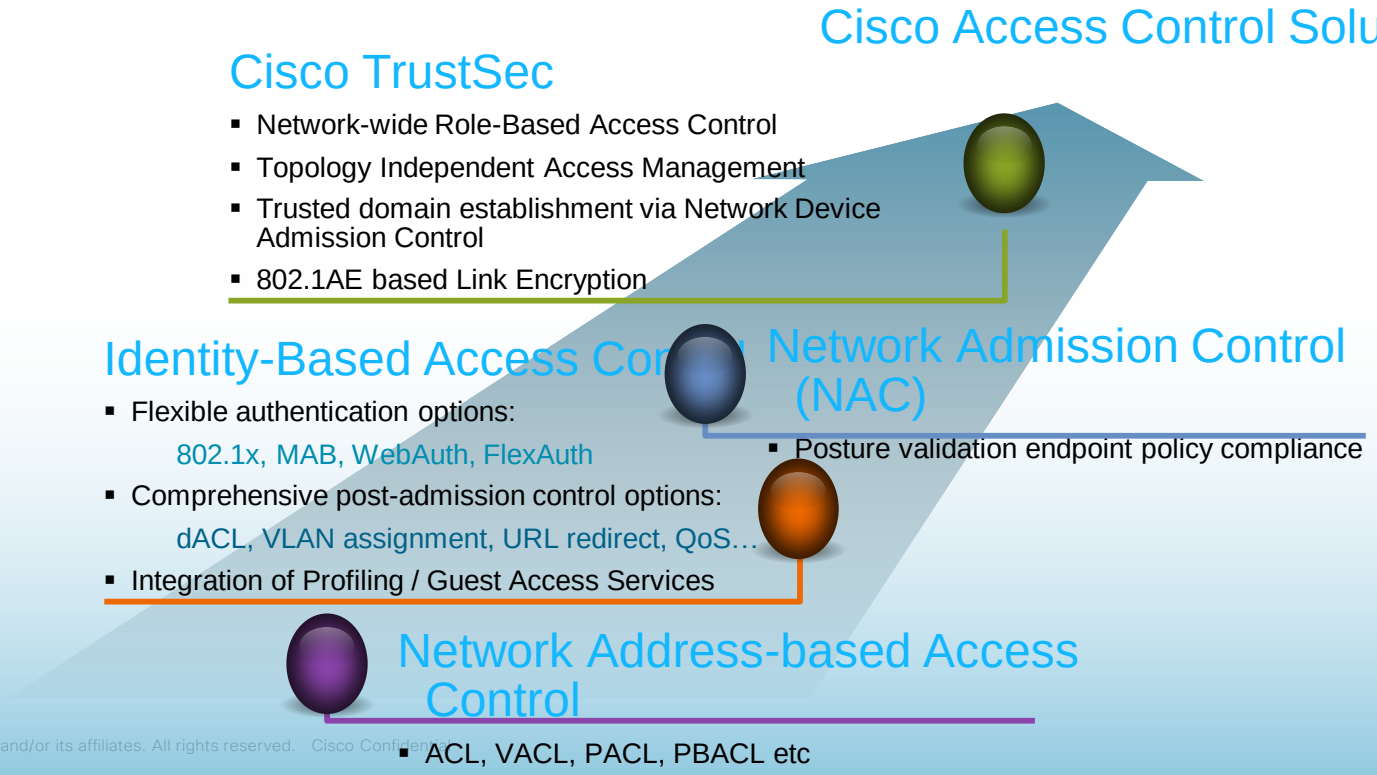


Preview of Posture Assessment by Condition

Logged At	Posture	Identity	Endpoint ID	IP Address	Endpoint OS	Policy	Enforcement	Condition Status
2015-04-01 12:23:45.270	✗	user	00:1A:A1:92:C3:BB	10.23.43.56	Windows 7 Ente	win7-MSE-Check	Mandatory	Failed
2015-04-01 12:23:45.270	✗	user1	00:1A:A1:92:C3:BB	10.23.43.56	Windows 7 Profe	optional_win_chk_copy	Optional	Skipped
2015-04-01 12:23:45.270	✓	Dev1	00:1F:29:71:8F:4C	192.168.123.17	Windows 7 Ente	Custom_checks	Mandatory	Passed

Using this report we can easily find the **non compliant devices**, with this report the field support team can solve the desktop issues quickly.

Controle de Acesso: Evolução



Pergunta 3

- Qual feature mitiga um ataque do tipo men-in-the-middle para o protocolo radius?

A. Macsec

B. DAI

C. DHCP Snooping

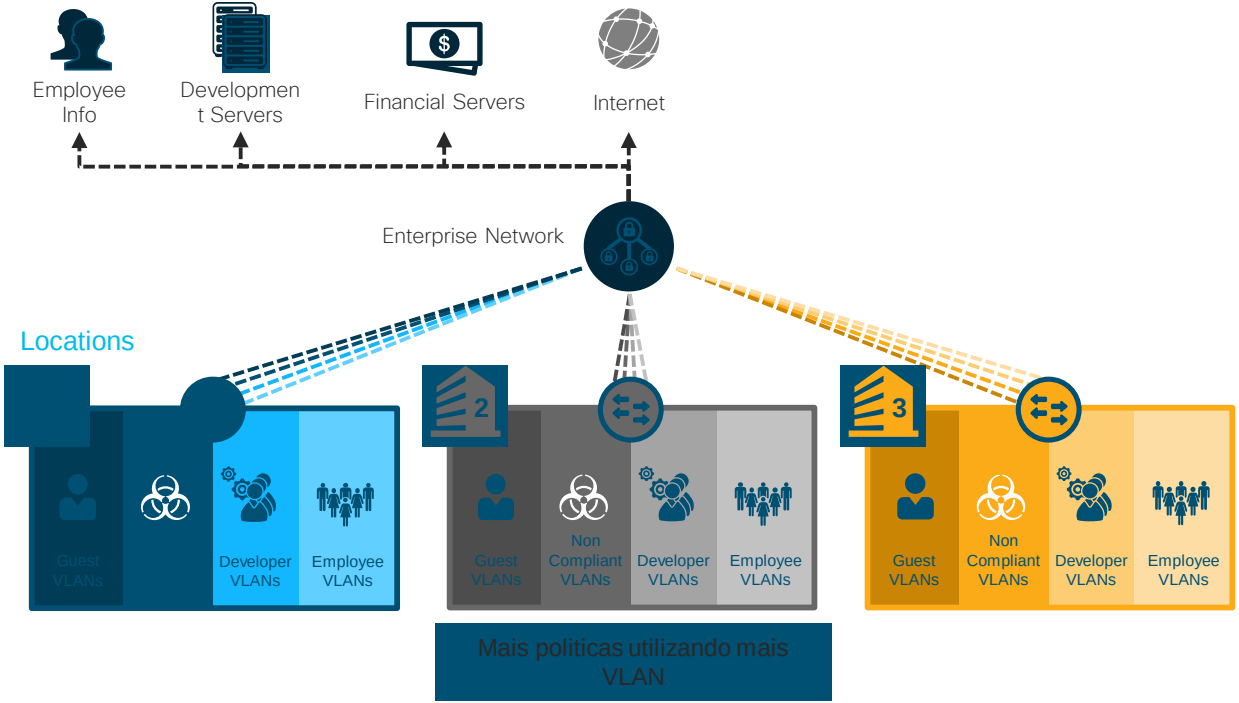
Segmentação Tradicional

Politicas de segurança baseadas em IP, resultando em:

Gerenciamento de acesso complicado

Configuração Manual, consumo de tempo, segurança e manutenção

Politicas inconsistentes em todos os dispositivos da rede



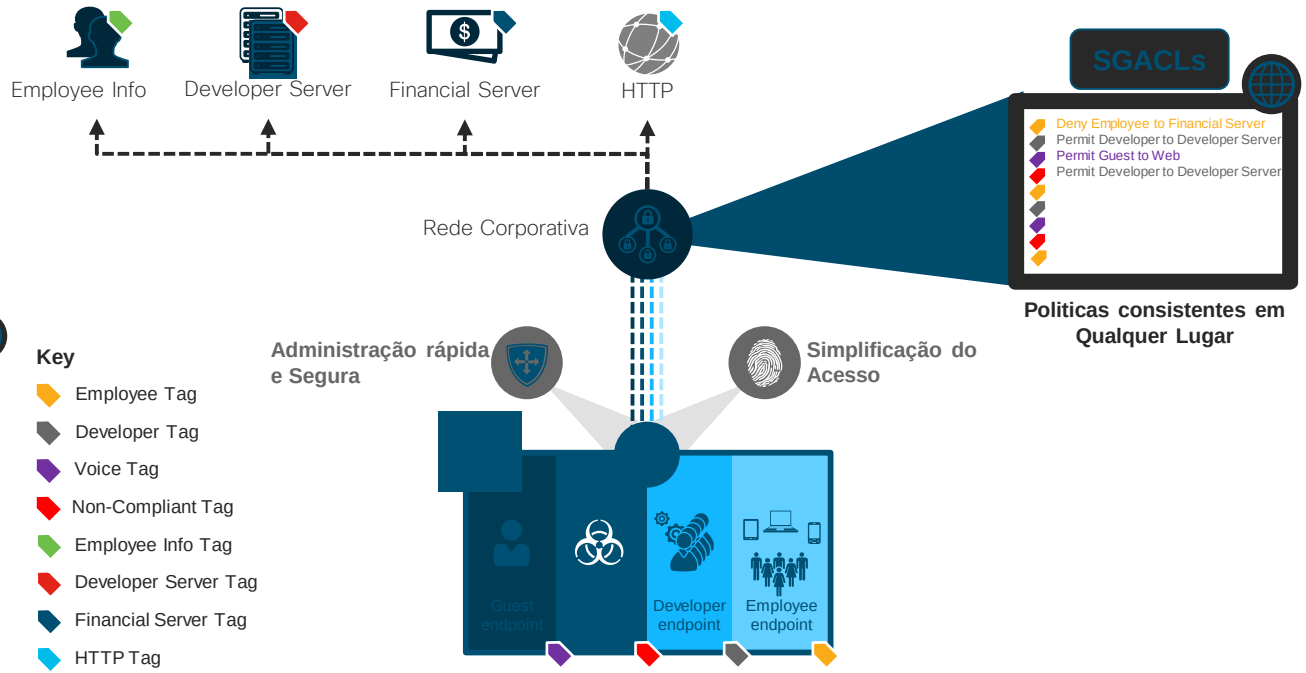
Utilizando a Solução de TrustSec

TrustSec simplifica o provisionamento dos dispositivos no acesso à rede, acelerando as operações de segurança de forma consistente. Esta segmentação tecnologia escalável e ágil é incorporado em mais de 40 switches, roteadores, dispositivos wireless e outros produtos Cisco

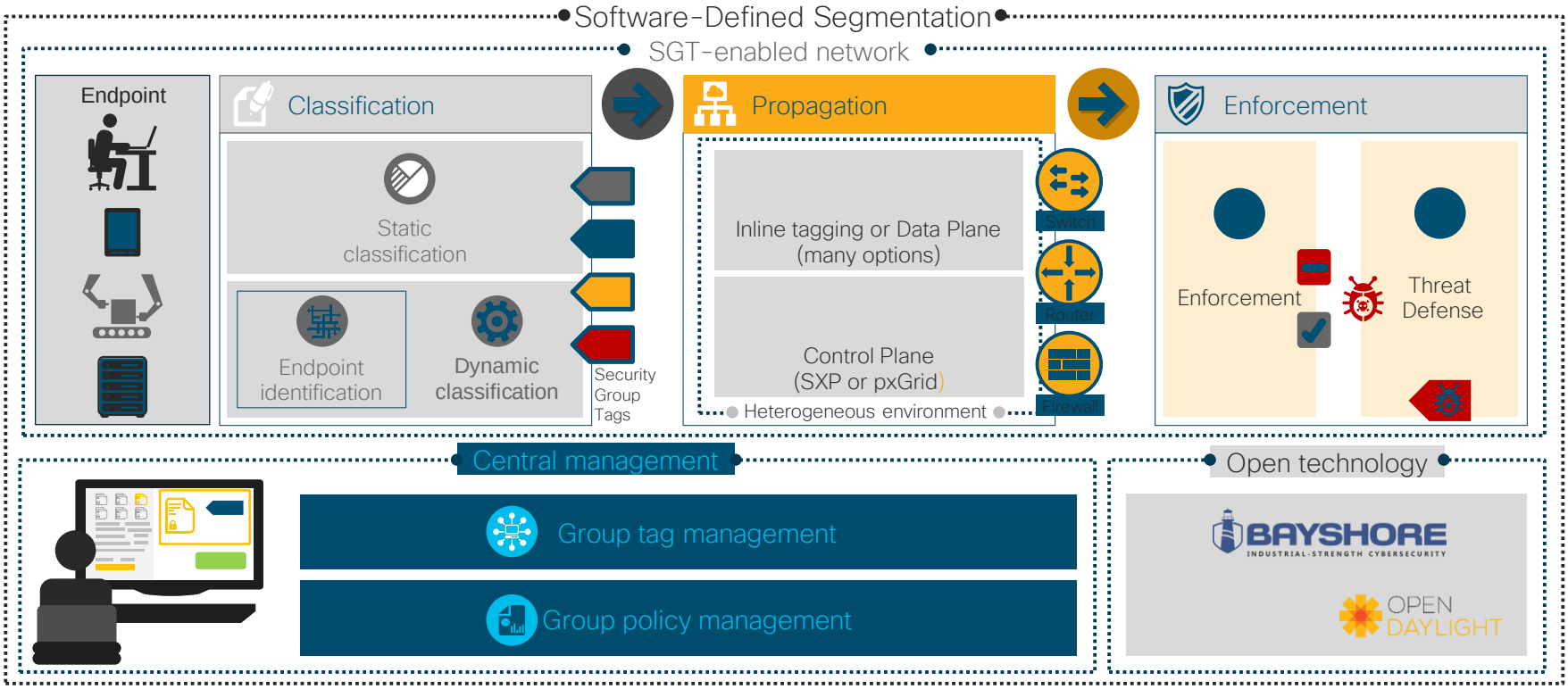
Simplificação do Acesso
Gerência as políticas utilizando uma linguagem simples e mantêm a conformidade através do controle de acesso com base na função

Administração rápida e Segura
Reduzir a necessidade de re-arquitetura de rede, automatizando a administração das regras de firewall e (ACL) acelerando o provisionamento dos serviços.

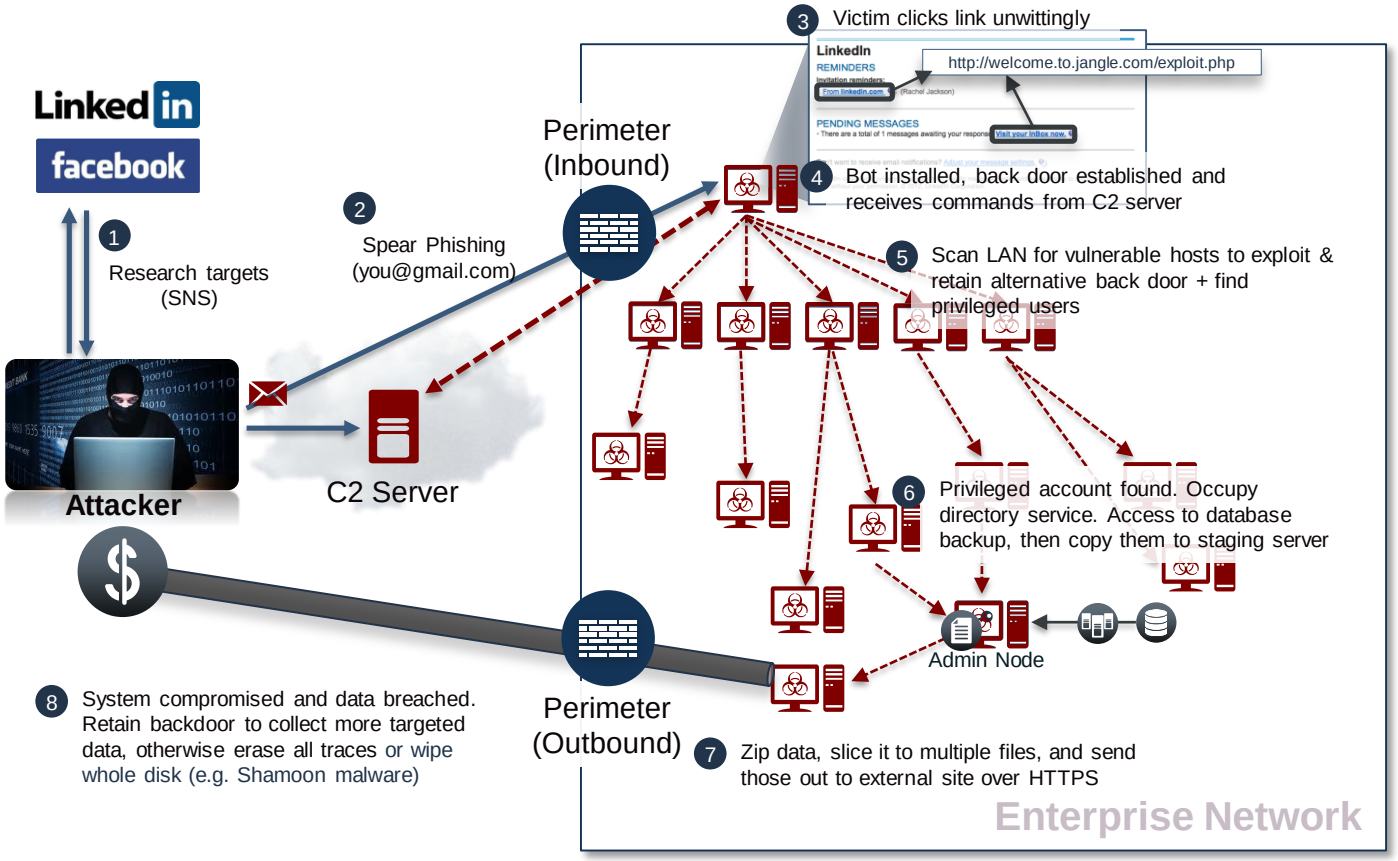
Politicas consistentes em Qualquer Lugar
Controla todos os segmentos de rede de forma centralizada, independente dos meios (Cabeada, Wireless ou VPN)



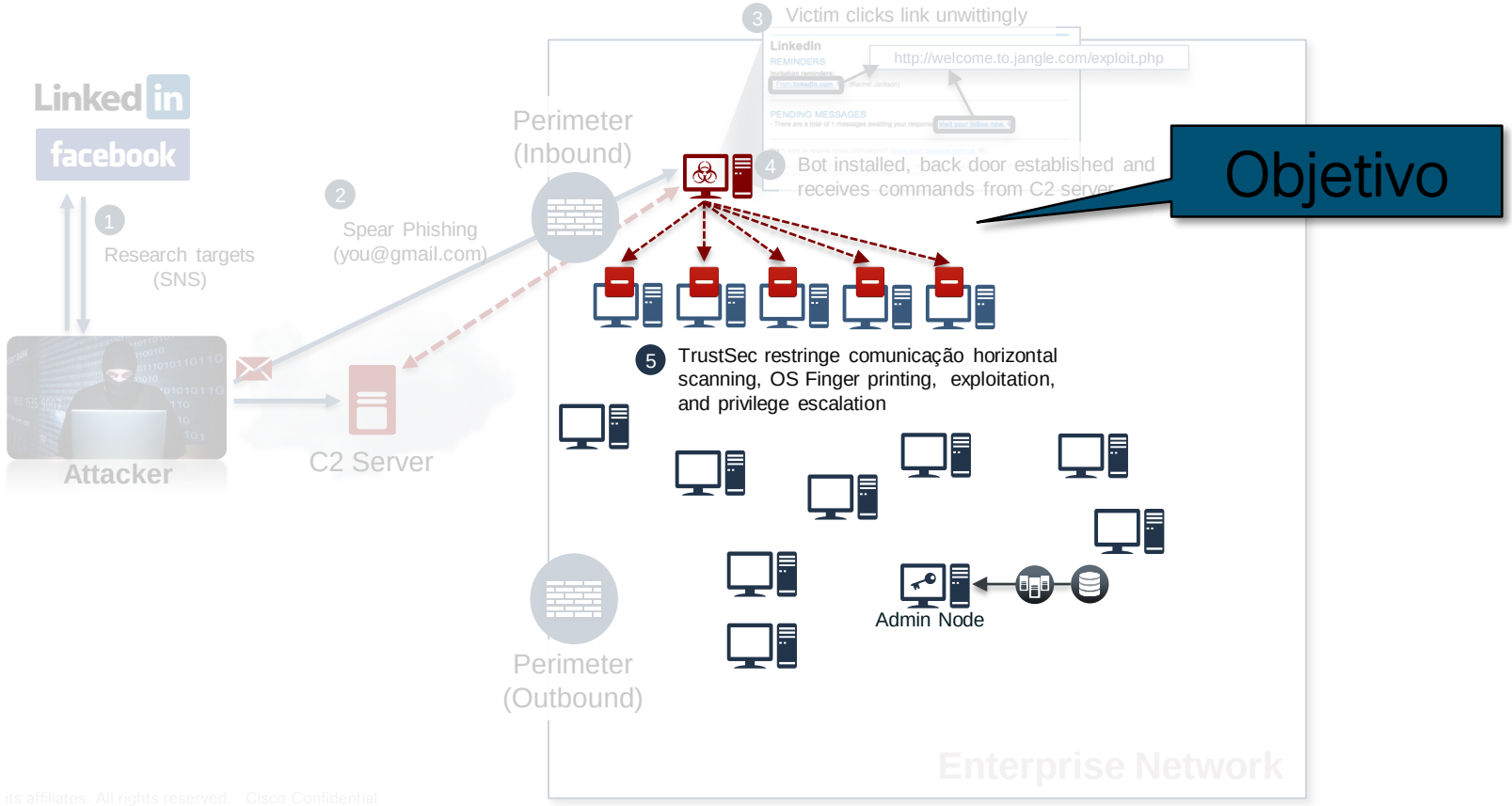
Processos do TrustSec



Processo de violação



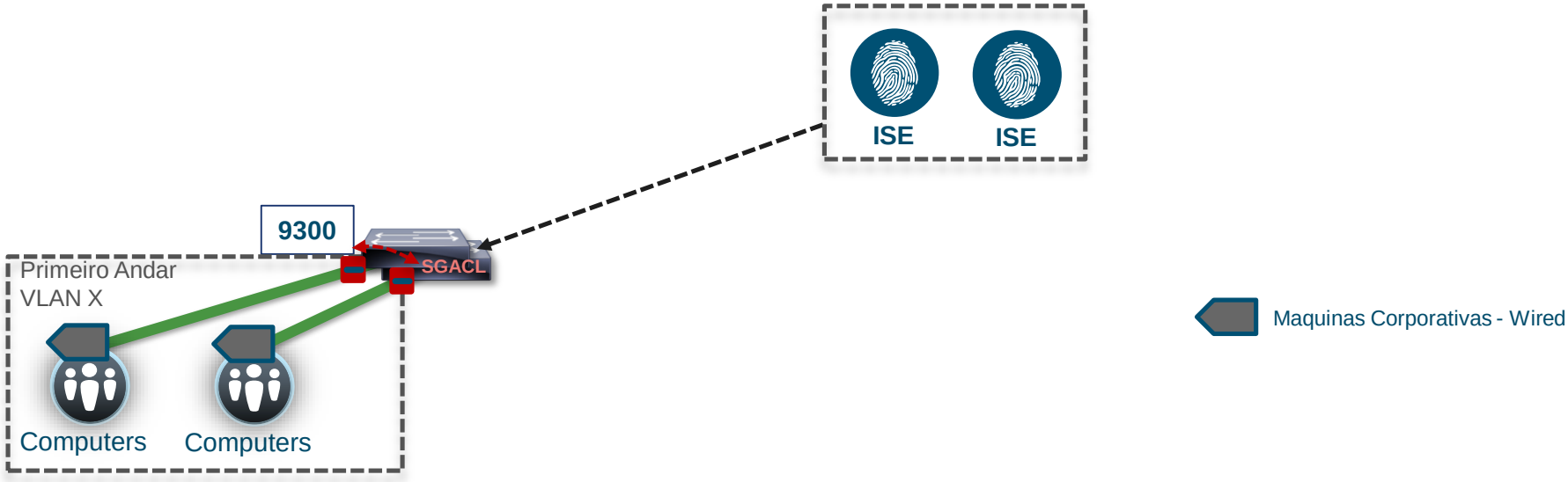
Proteção com TrustSec



Use Case 1 – TrustSec (Mesmo Stack)

Micro segmentação horizontal (9300)

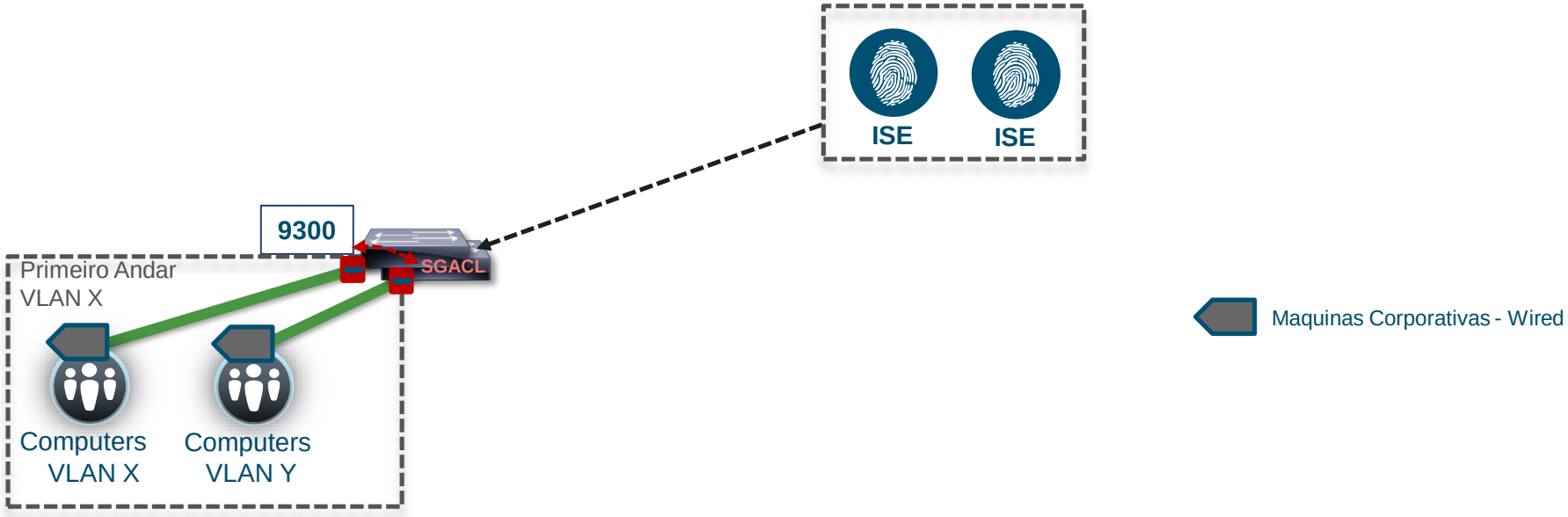
- **Atividades:**
  - Micro segmentação lateral de maquinas na mesma pilha de switches (9300) – **Mesma VLAN**;



Use Case 2 – TrustSec (Mesmo Stack)

Micro segmentação horizontal (9300)

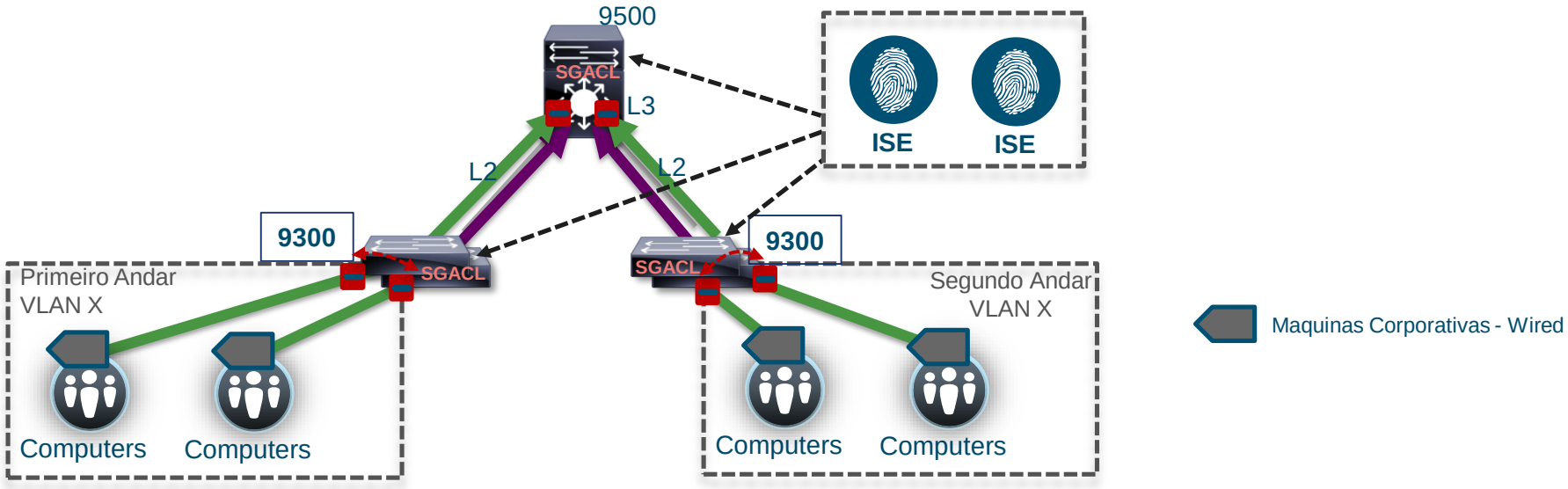
- **Atividades:**
  - Micro segmentação lateral de maquinas na mesma pilha de switches (9300) – **VLAN diferente**;



Use Case 3 – TrustSec (Diferentes Stacks)

Micro segmentação horizontal usando o switch de distribuição (9500)

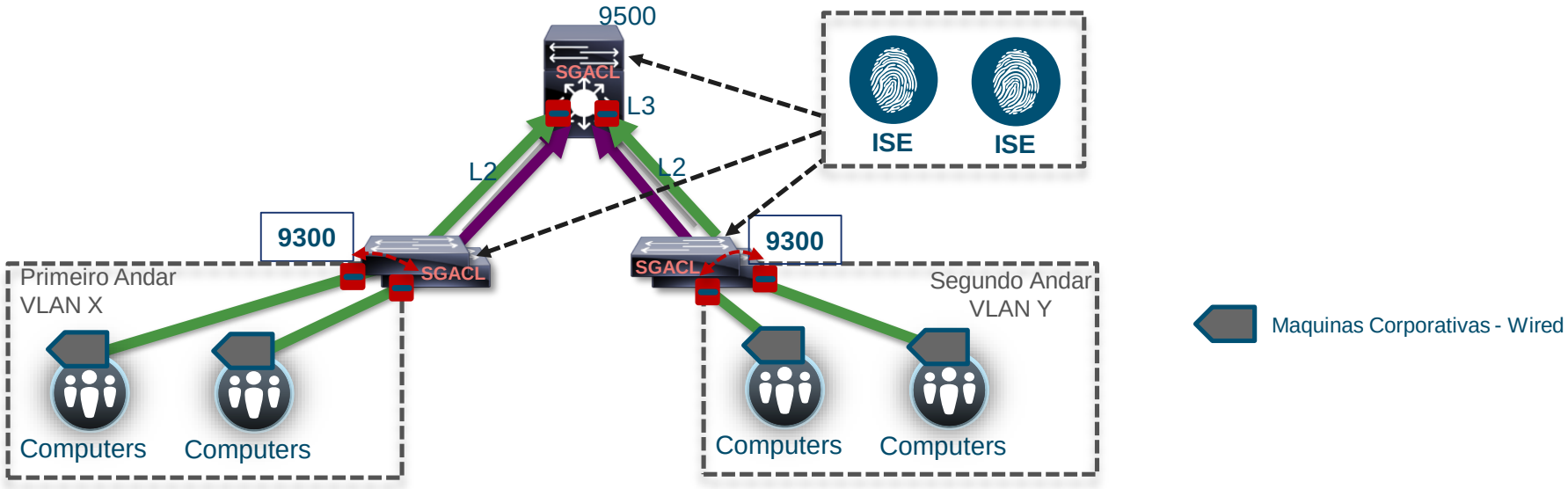
- **Atividades:**
  - Micro segmentação de maquinas em pilhas de switches distintas (9300 x 9500)
  - **Mesma VLAN**



Use Case 4 – TrustSec (Diferentes Stacks)

Micro segmentação horizontal usando o switch de distribuição (6500)

- **Atividades:**
  - Micro segmentação de maquinas em pilhas de switches distintas (9300 x 9500)
  - **VLAN diferente**



TrustSec
Modelo de Role Based ACL – Corporate Computers / Device IoT

- **Policy Matrix:**

	Domain Computers	Devices-IoT
Domain Computers	SGACL-1	DENY
Device-IoT	DENY	SGACL-2

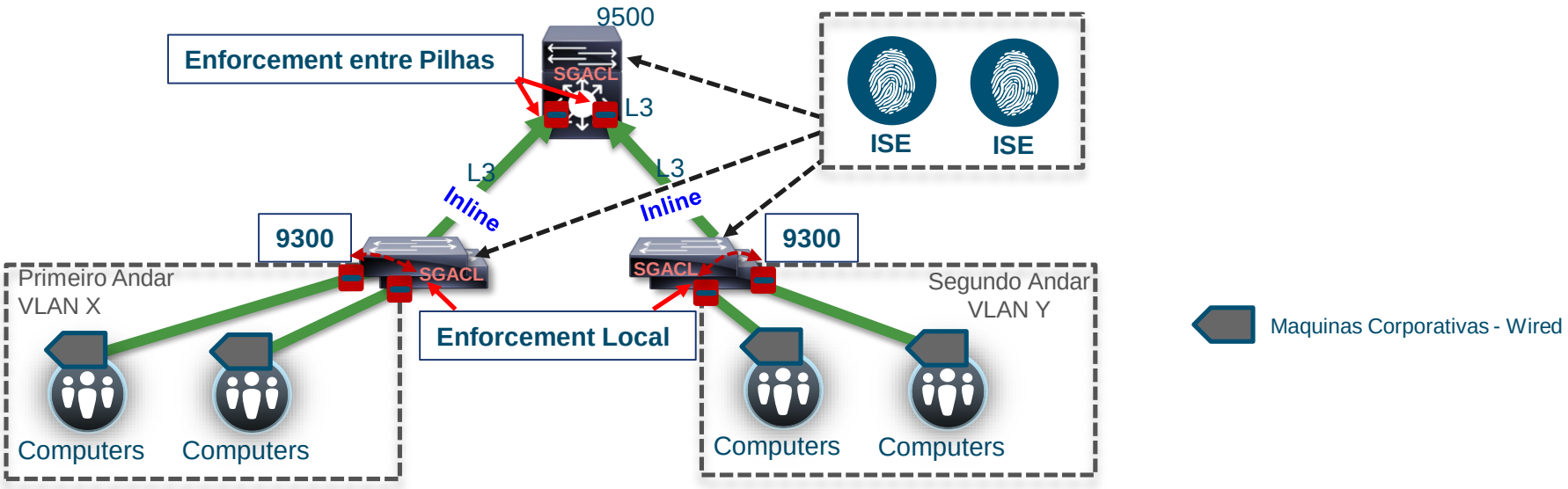
Restrict ACL SGACL-2 (IoT)

```
permit  icmp
deny    udp src dst eq domain
deny    tcp src dst eq 3389
deny    tcp src dst eq 1433
deny    tcp src dst eq 1521
permit ip
```

Restrict SGACL-1 (Corporate)

```
permit  icmp
deny    udp src dst eq domain
deny    tcp src dst eq 3389
deny    tcp src dst eq 1433
deny    tcp src dst eq 1521
deny    tcp src dst eq 445
deny    tcp src dst eq 137
deny    tcp src dst eq 138
deny    tcp src dst eq 139
deny    udp src dst eq snmp
deny    tcp src dst eq telnet
deny    tcp src dst eq www
deny    tcp src dst eq 443
deny    tcp src dst eq 22
deny    tcp src dst eq pop3
deny    tcp src dst eq 123
deny    tcp match-all -ack +fin -psh -rst -syn -
urg
deny    tcp match-all +fin +psh +urg
permit ip
```

Design Proposto
Propagação utilizando Inline tag



Design Proposto
Propagação utilizando Inline tag

Origem/Destino	SGT Domain computers	SGT DEVICE MAB	SGT DEVICE IoT	SGT Excecao Grupo AD	Unknown
SGT Domain computers	SGACL-1	SGACL-1	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY
SGT DEVICE MAB	SGACL-1	SGACL-1	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY
SGT DEVICE IoT	SGACL-DENY-ANY	SGACL-DENY-ANY	SGACL-2	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY
SGT Excecao Grupo AD	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY
Unknown	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY	SGACL-PERMIT-ANY

Faça suas perguntas agora!

Use o painel
Perguntas e Respostas ou Q&A
para enviar suas perguntas.

Nosso especialista responderá ao vivo

Notícias e eventos futuros

http://bit.ly/eventosdacomunidade

Pergunte ao especialista após o Webcast

Além do evento de hoje, se poderá fazer mais perguntas sobre: Mitigação de ataques em redes de computadores utilizando 802.1X, TrustSec e MacSec

Até a próxima sexta-feira, 13 de setembro de 2019.

Clique aquí para participar: https://community.cisco.com/t5/eventos-de-seguran%C3%A7a/pergunte-ao-especialista-evento-mitiga%C3%A7%C3%A3o-de-ataques-em-redes-de/ba-p/3918534

Luis Matos
Arquiteto de Soluções

Diga adeus aos eventos
“Webcasts” e “Pergunte ao especialista”
como você os conhece hoje!

Diga olá aos novos eventos
“Community Live” e “Ask Me Anything".

Saiba mais aqui: https://community.cisco.com/t5/blogues-de-geral/os-eventos-da-comunidade-cisco-est%C3%A3o-recebendo-um-novo-nome/ba-p/3916998

Participe em nossas Redes sociais

Twitter

- @Cisco_Support
- @CiscoDoBrasil

Facebook

- Hey Cisco

http://bit.ly/csc-facebook

- Cisco Do Brasil

https://www.facebook.com/CiscoDoBrasil/

- Cisco Portugal

https://www.facebook.com/ciscoportugal/

Saiba mais sobre os próximos eventos

Convidamos você a visitar nossas canais

YouTube

- Cisco Comunity
- http://bit.ly/csc-youtube

App

- Cisco Technical Support

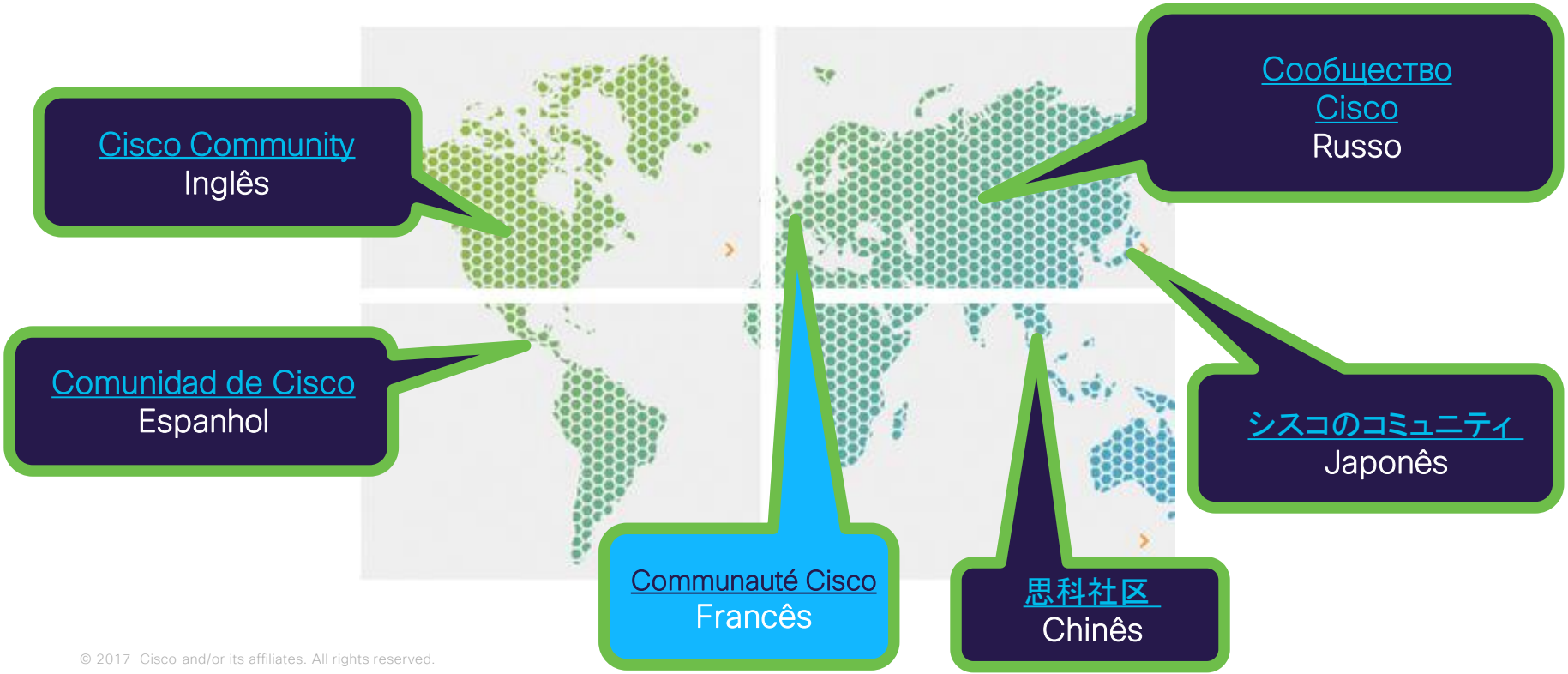
LinkedIn

- Cisco-Community
- http://bit.ly/csc-linked-in

Saiba mais sobre os próximos eventos

A Cisco também tem Comunidades em outros idiomas!

Se você fala Inglês, Espanhol, Francês, Japonês, Russo ou Chinês, lhe convidamos a conhecer nossas Comunidades



Obrigado por sua participação

Por favor, tome 10 segundos para responder nossa enquete de múltipla escolha ao finalizar o evento!

Sua opinião é muito importante para continuar melhorando!

Obrigado por ser parte dessa experiência


CISCO