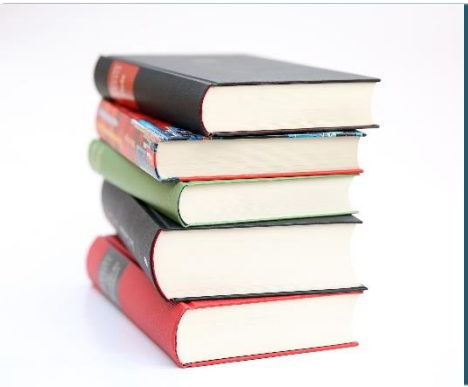
Kapitola 10: Pokročilé ovládanie ASA cez ASDM GUI

CCNA Security v2.0



Obsah kapitoly

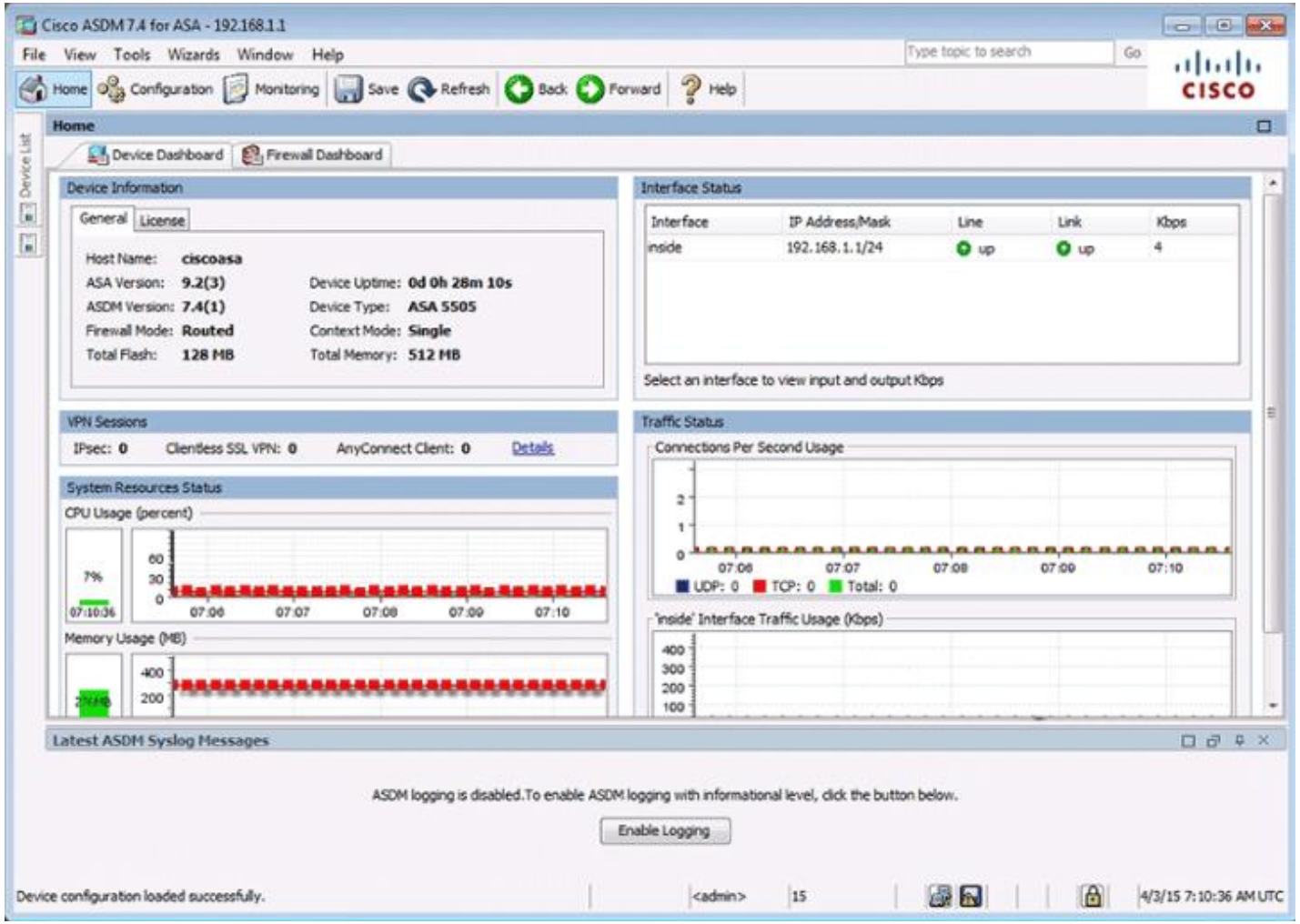
- 10.0 Úvod
- 10.1 ASA Security Device Manager (ASDM)
- 10.2 Konfigurácia ASA VPN
- 10.3 Zhrnutie

Úvod

- Adaptívne bezpečnostné zariadenie (ASA) Cisco poskytuje:
  - Komplexné firewall-ové riešenia (s FirePower)
  - Škálovateľnosť
  - Je súčasťou Cisco Secure Borderless Network
- Skupinu firewallov ASA 5500 je možné ovládať dvoma spôsobmi:
  - Príkazovým riadkom (CLI)
    - Rýchle, ale pre advanced users
  - Grafickým rozhraním - ASA Security Device Manager (ASDM)
    - Pomalší spôsob

ASDM - ASA Security Device Manager

- Java-Based GUI
- Browserová alebo desktopová aplikácia
  - Umožňuje setup nastavenie, konfiguráciu, monitorovanie, troubleshooting
    - ASA Packet Tracer ☺
  - Spojenie cez SSL certifikát



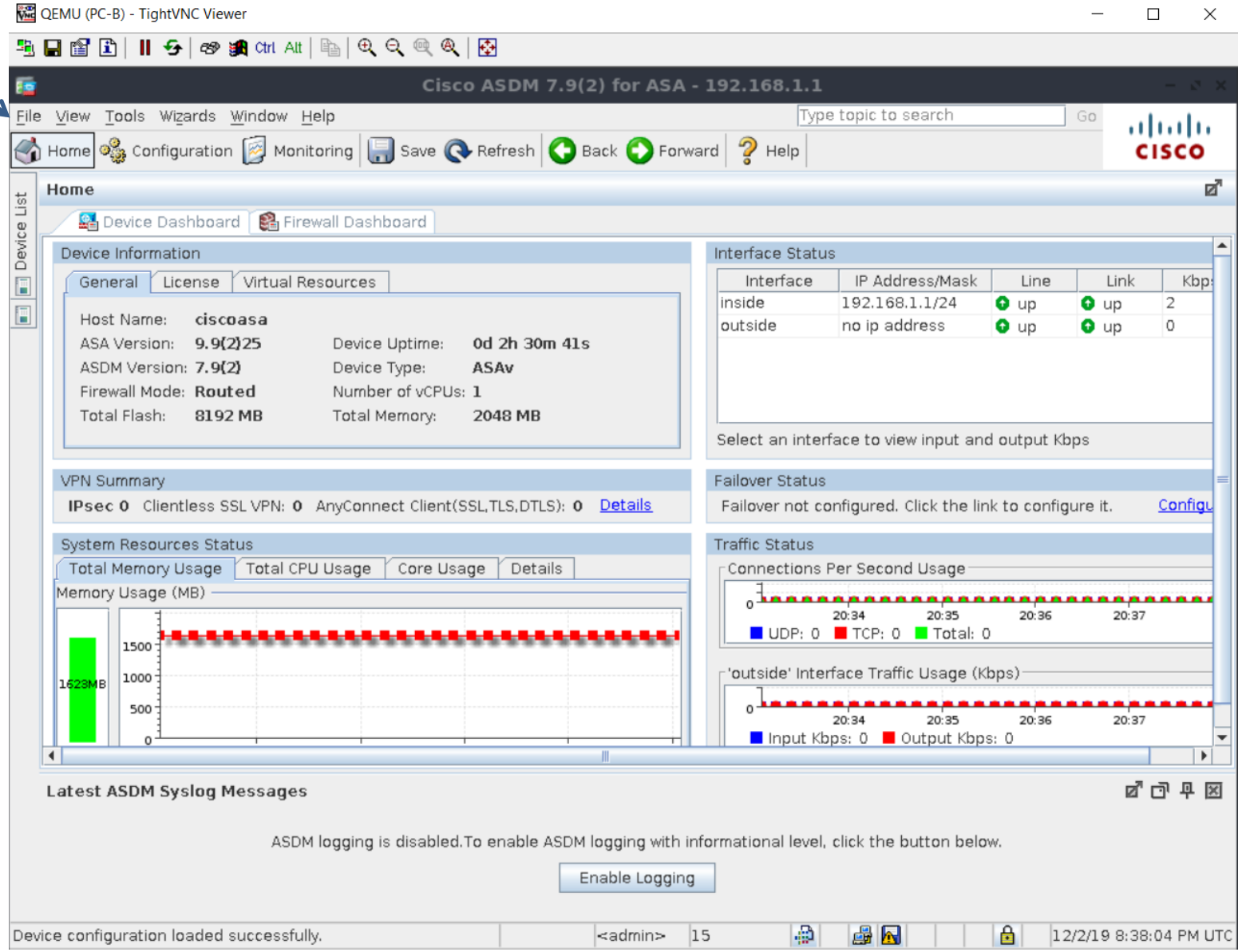
Domovské menu - ASDM dashboard

Menu bar

Tool bar

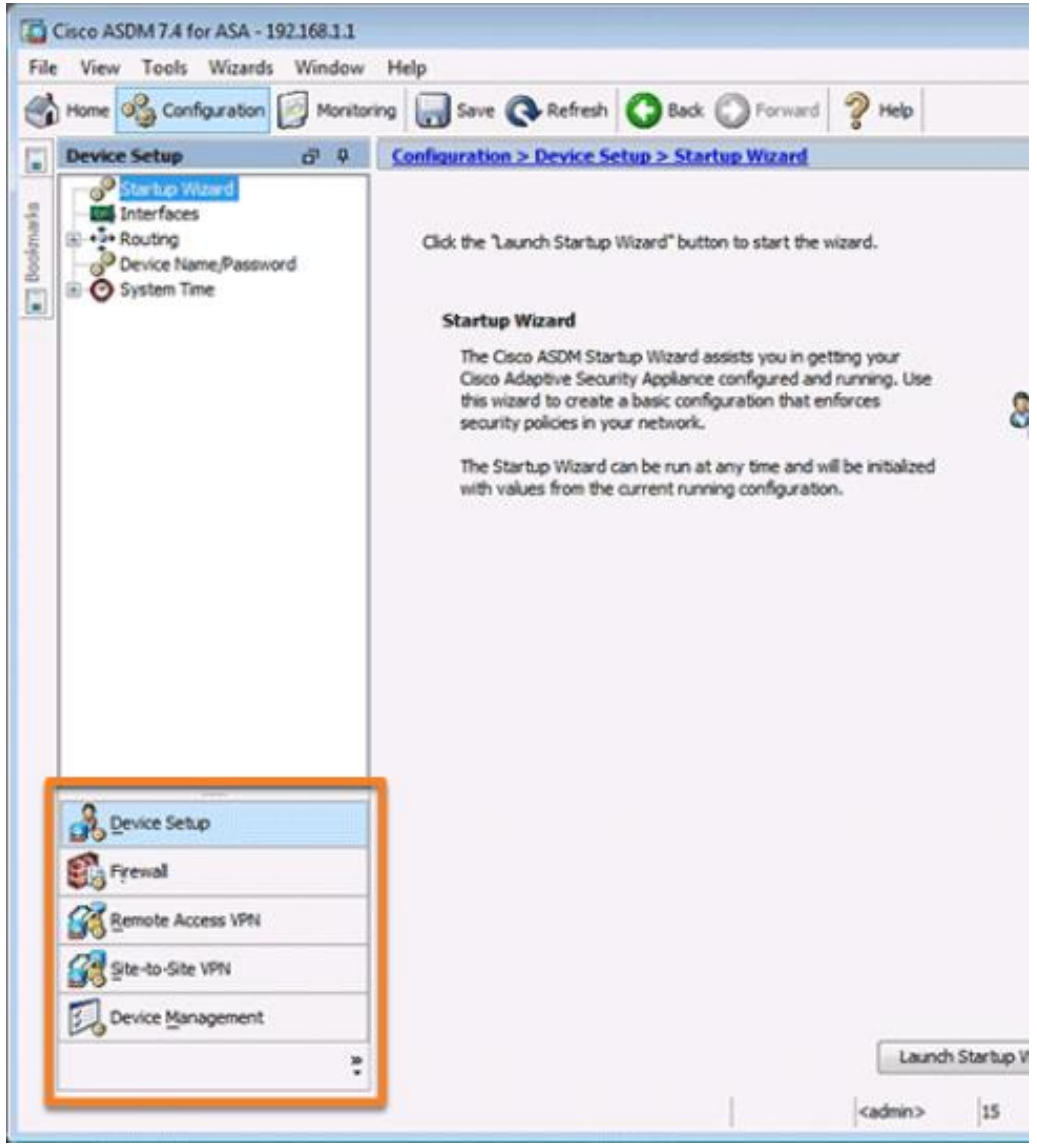
Device list

Status bar

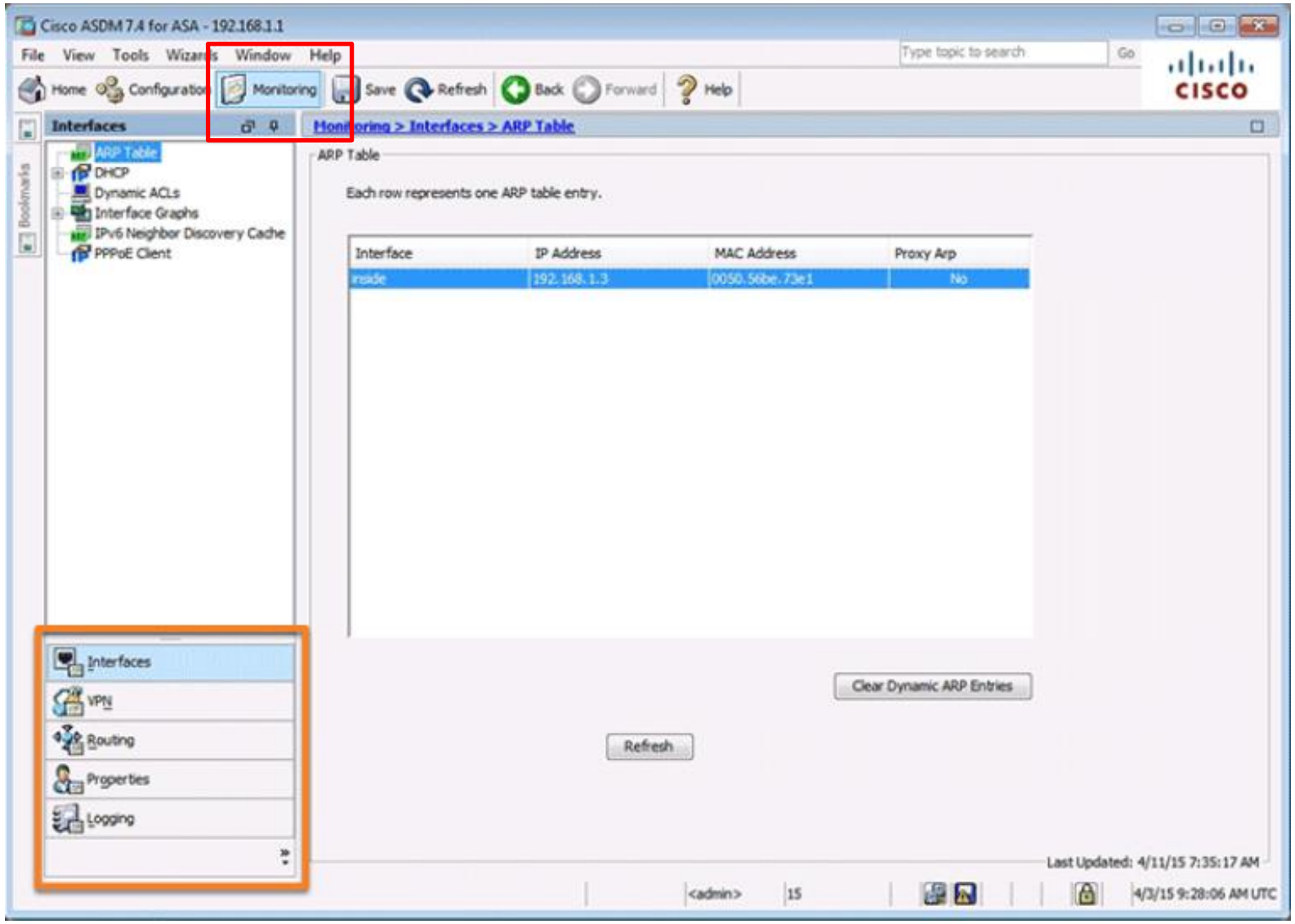


Domovské menu - ASDM dashboard

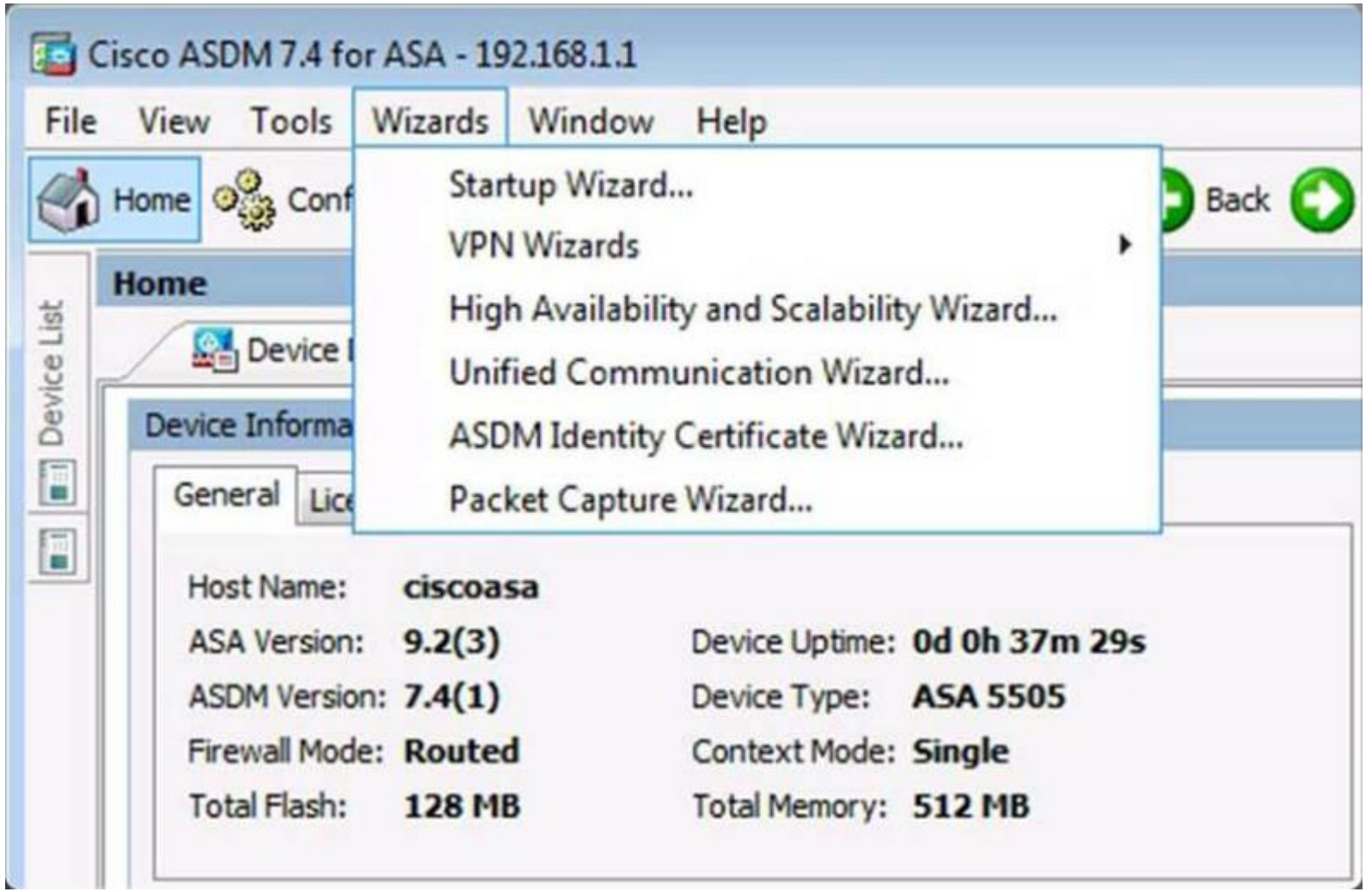
- Tool bar => configuration
  - Prístup ku konfiguračným voľbám ASA
    - Device setup
    - Firewal konfig
    - Remote Access VPN konfig
    - Site to site VPN konfig
    - Device management konfig
  - Pozor: zmeny treba vždy ukladať



ASDM – monitoring view



ASDM – config wizards



10.1 ASA Security Device Manager (ASDM)

Po dokončení tejto podkapitoly by ste mali vedieť nakonfigurovať:

- Prístup na ASDM
- Základné nastavenia ASA prost. ASDM (rozhrania, DHCP, SSH, PAT/NAT...)
- Dodatočné nastavenia ASA prostr. ASDM (AAA, DMZ, ACL)

Konfigurácia prístupu na 5505 pre ASDM

- Na ASA nakonfigurujte:
  - Vnútorné rozhranie vlan1
    - Názov rozhrania: inside (nameif inside)
    - IP adresa: 192.168.1.1/24
    - Security level na hodnotu 100 (security-level 100)
    - no shutdown
  - Povoľte HTTPS prístup na ASA zo siete 192.168.1.0/24 (http server enable, http 192.168.1.0 255.255.255.0 inside)

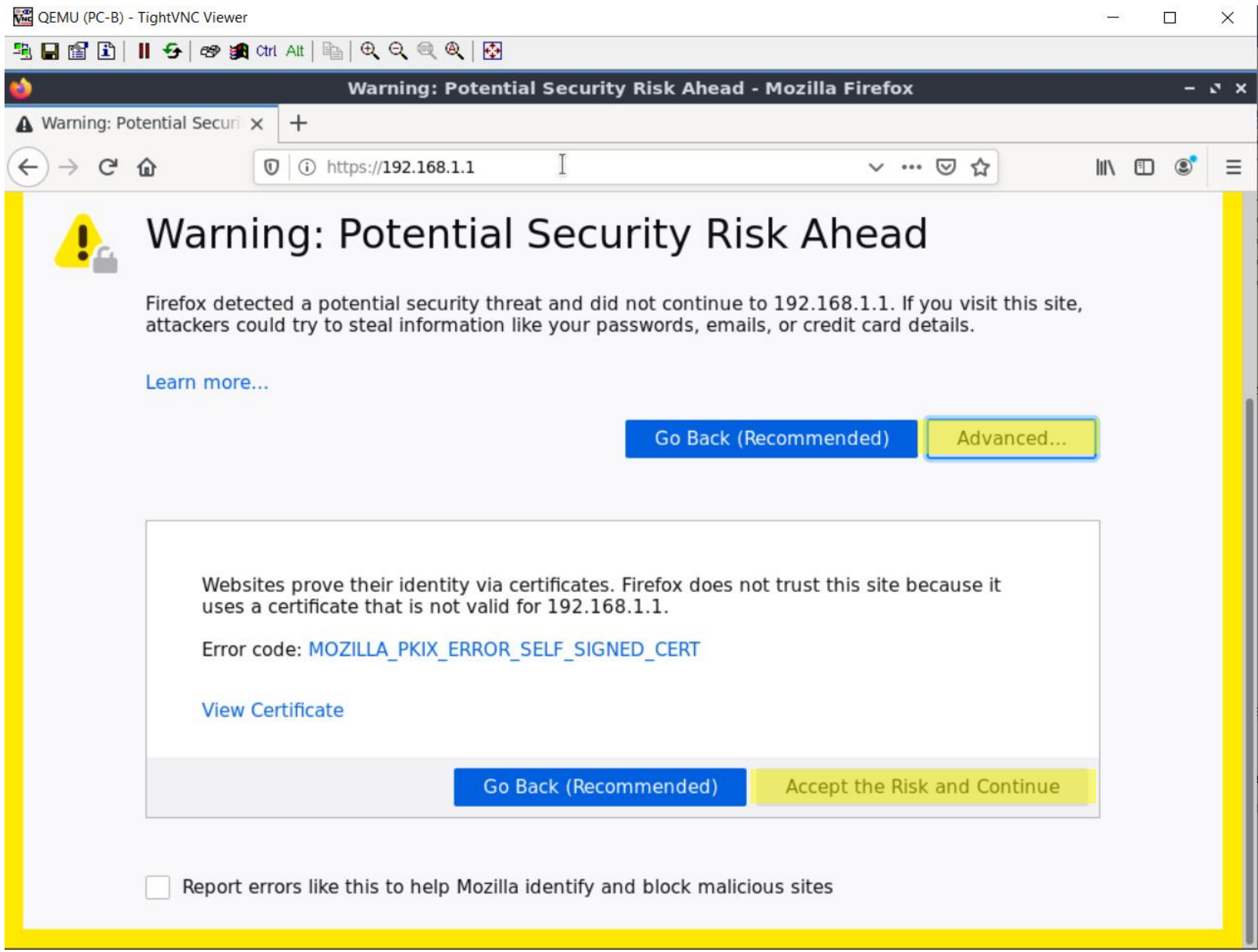
```
ciscoasa# conf t
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.3 255.255.255.255 inside
ciscoasa(config)#
```

2. časť: Konfigurácia prístupu na ASDM pre ASAv

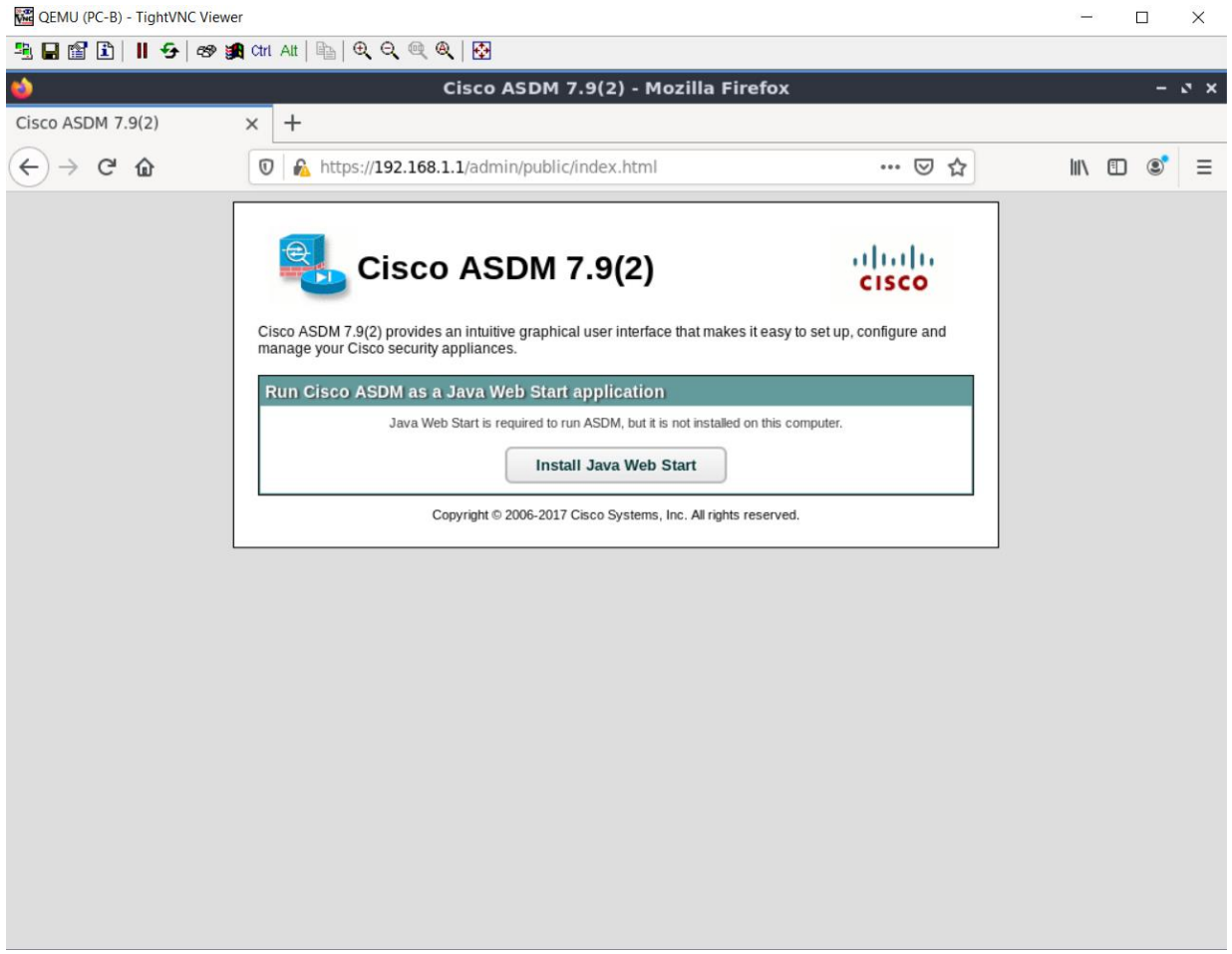
- Na ASA nakonfigurujte:
  - Vnútorné rozhranie Gi0/1
    - Názov rozhrania: inside (nameif inside)
    - IP adresa: 192.168.1.1/24
    - Security level na hodnotu 100 (security-level 100)
    - no shutdown
  - Vonkajšie rozhranie Gi0/2
    - Názov rozhrania: outside (nameif outside)
    - Security level na hodnotu 0 (security-level 0)
    - no shutdown
  - Povoľte HTTPS prístup na ASA zo siete 192.168.1.0/24 (http server enable, http 192.168.1.0 255.255.255.0 inside)
  - Username?

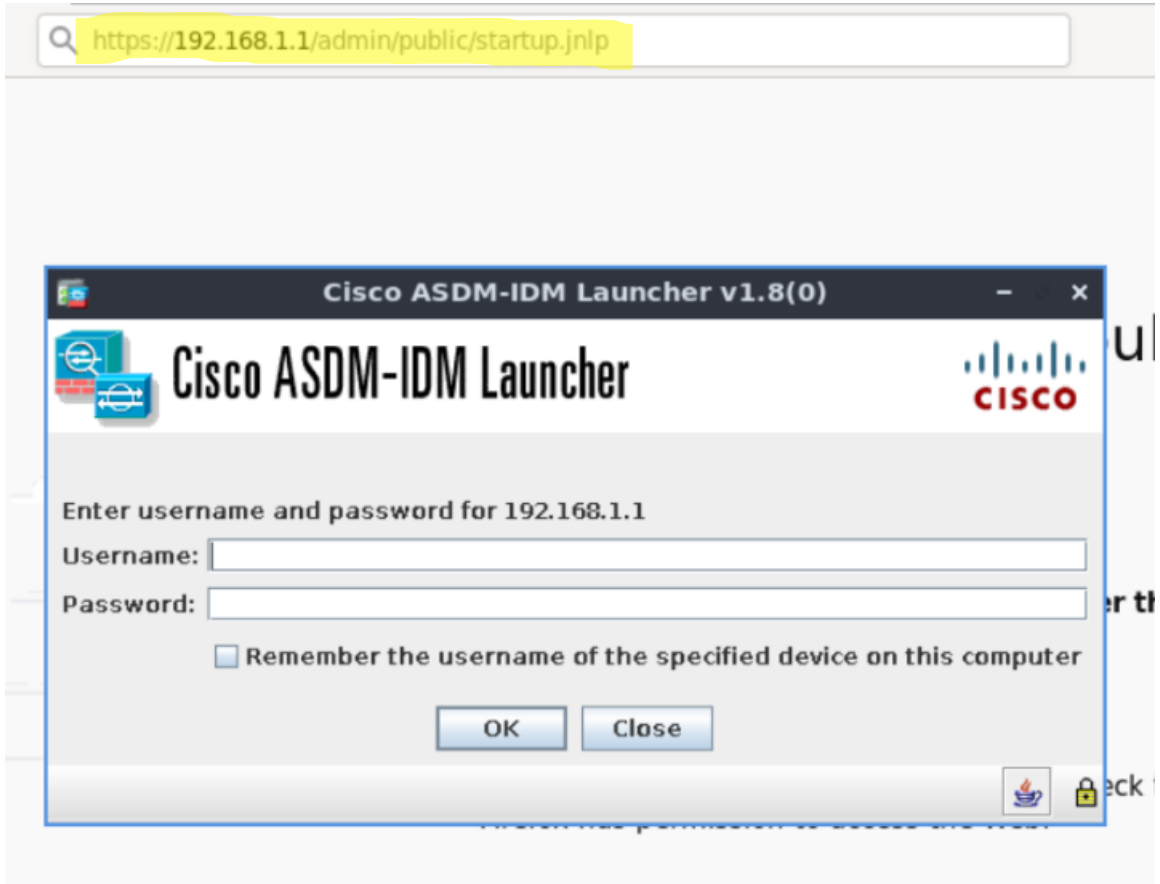
Prístup na ASDM

- Prehliadač
  - URL na IP adresu vnútorného rozhrania
  - Note: ASA používa self signed certs, nutné akceptovať *risk warnings*



Prístup na ASDM



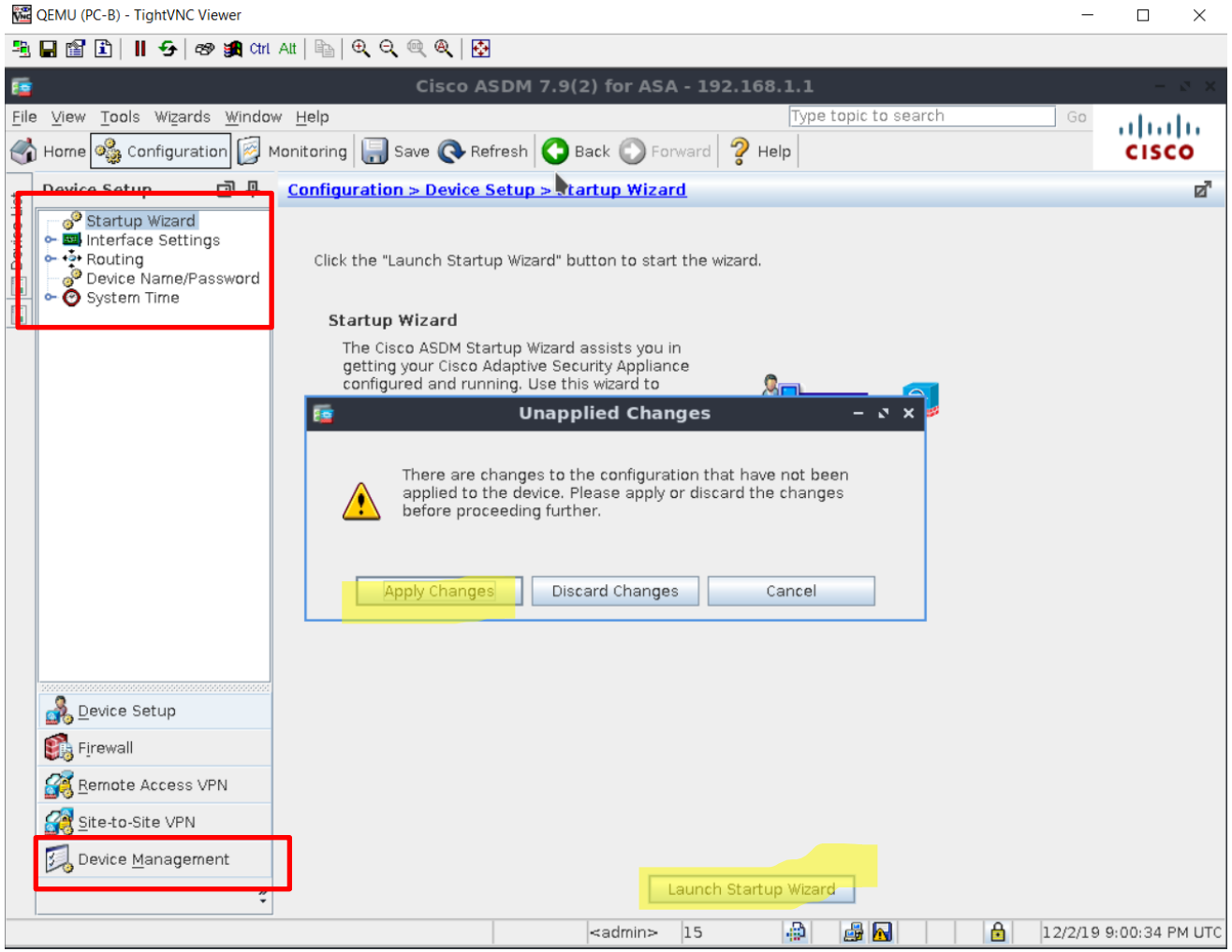


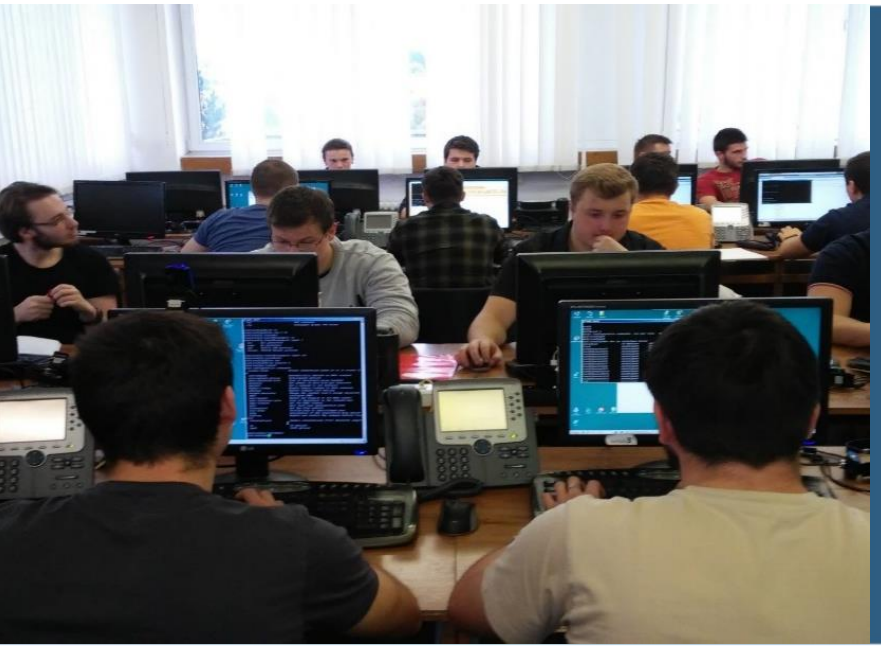
ASDM Security Warning - 1

ASDM Security Warning - 2

3. časť: Konfigurácia zákl. nastavení ASA cez ASDM

- Configuration
  - Device setup
    - => Startup wizard
    - Interface setting
    - Routing
    - Service passwords
    - System time
  - Device management
- Wizards => Startup wizard

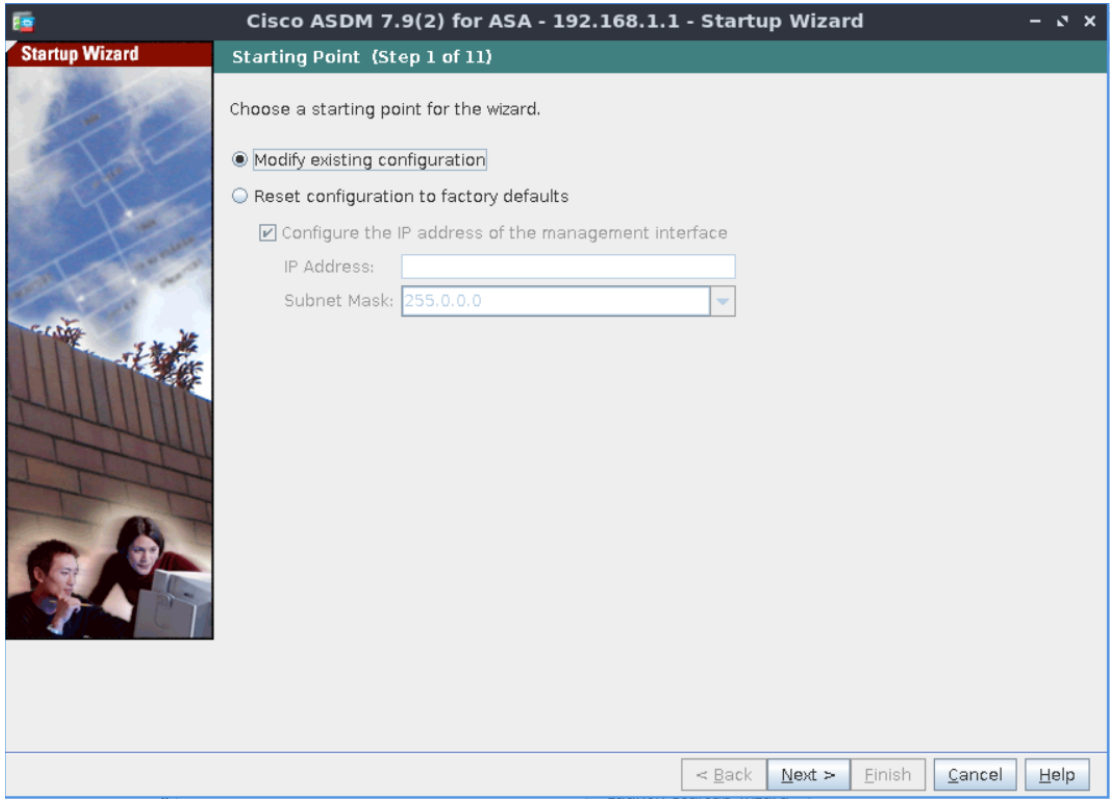




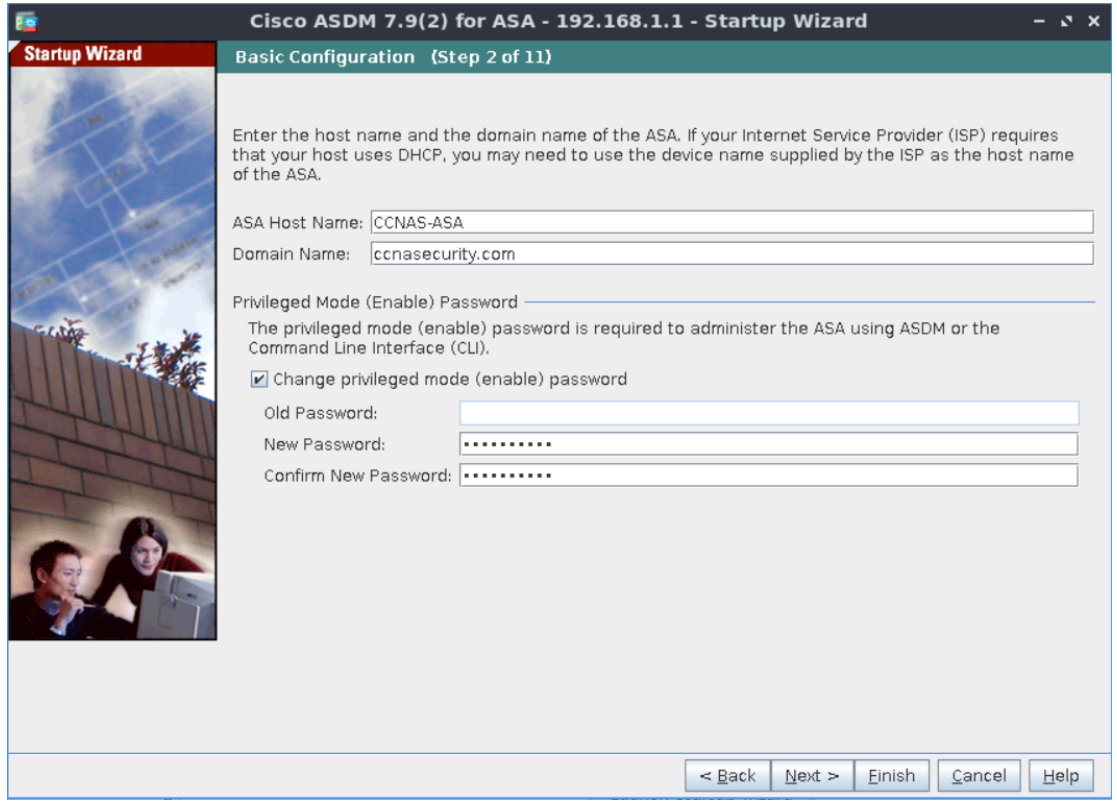
Základná konfigurácia => Wizards

Nastavenie ASA host name, domain name a hesla do privilegovaného módu

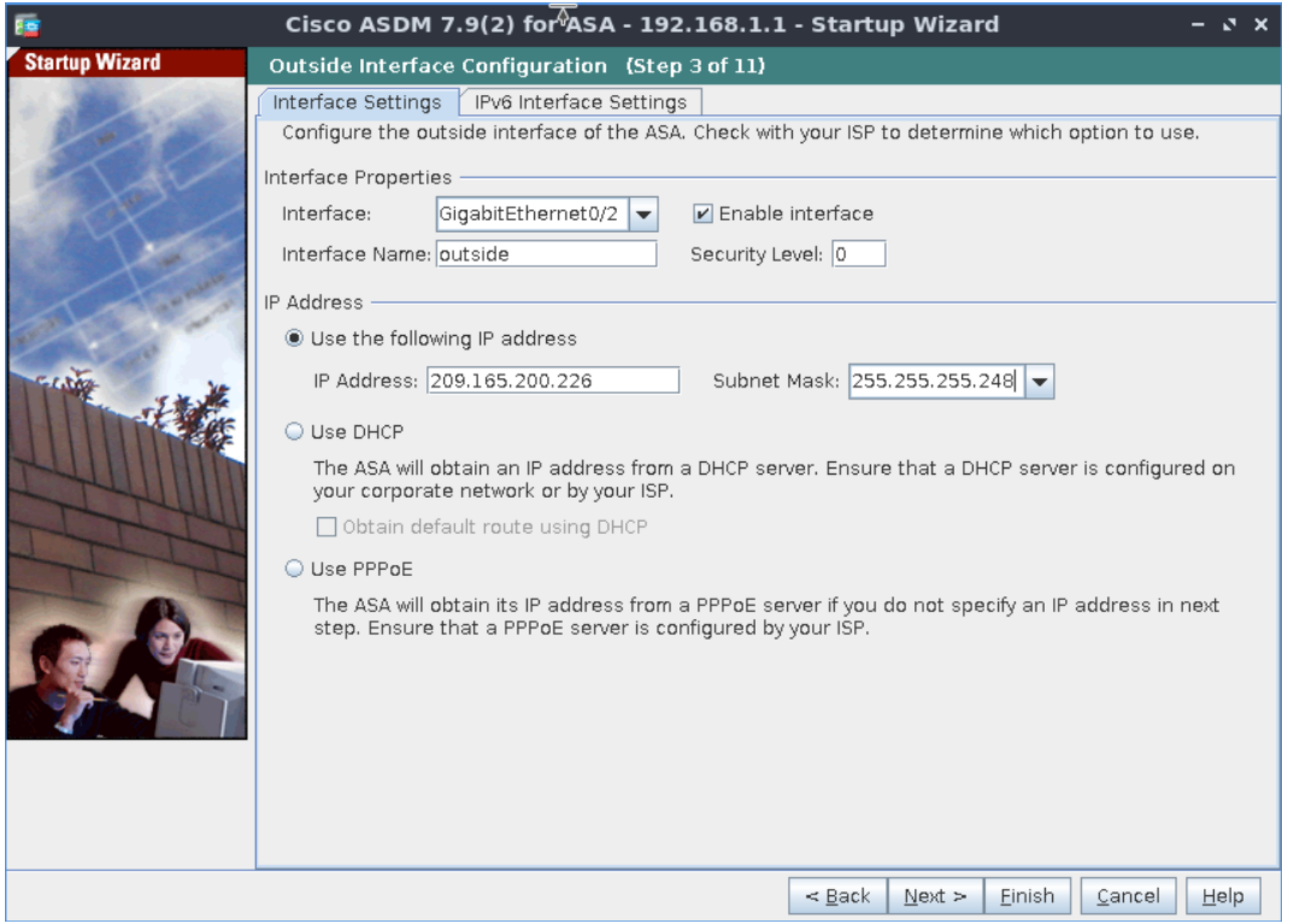
Startup Wizard Starting Point Window



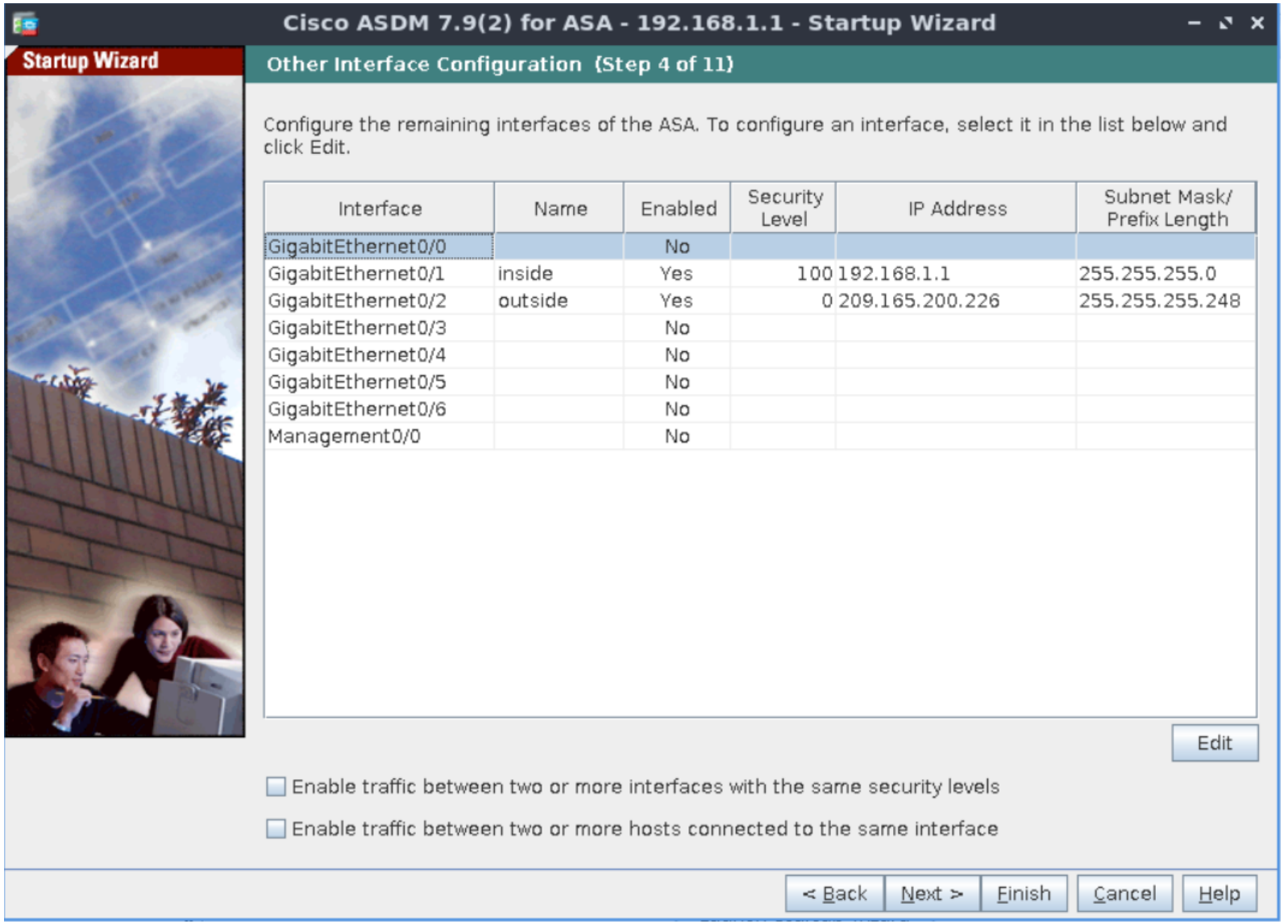
Startup Wizard Basic Configuration Window



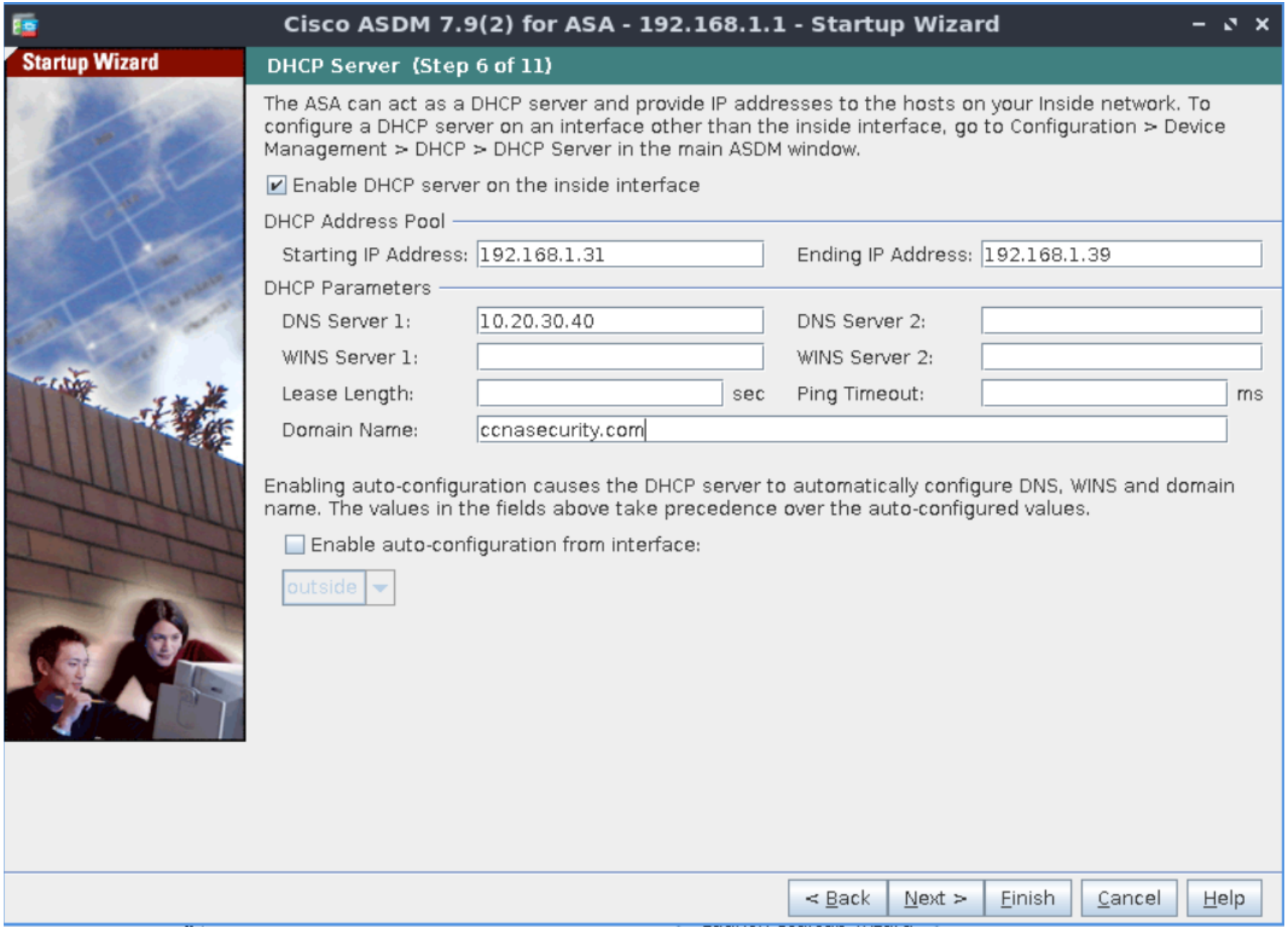
Konfigurácia vonkajšieho rozhrania



Kontrola vonkajšieho rozhrania

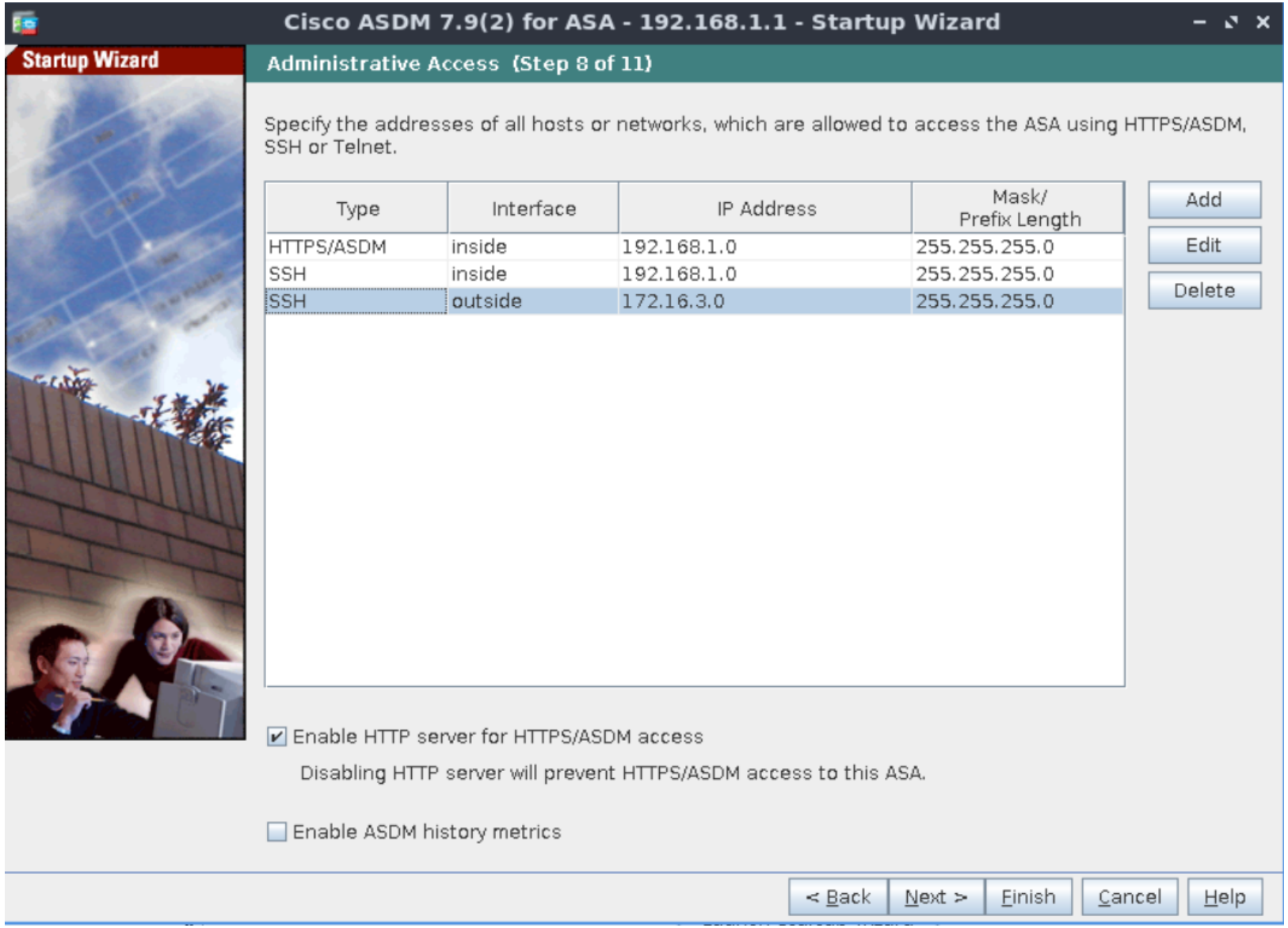


DHCP server

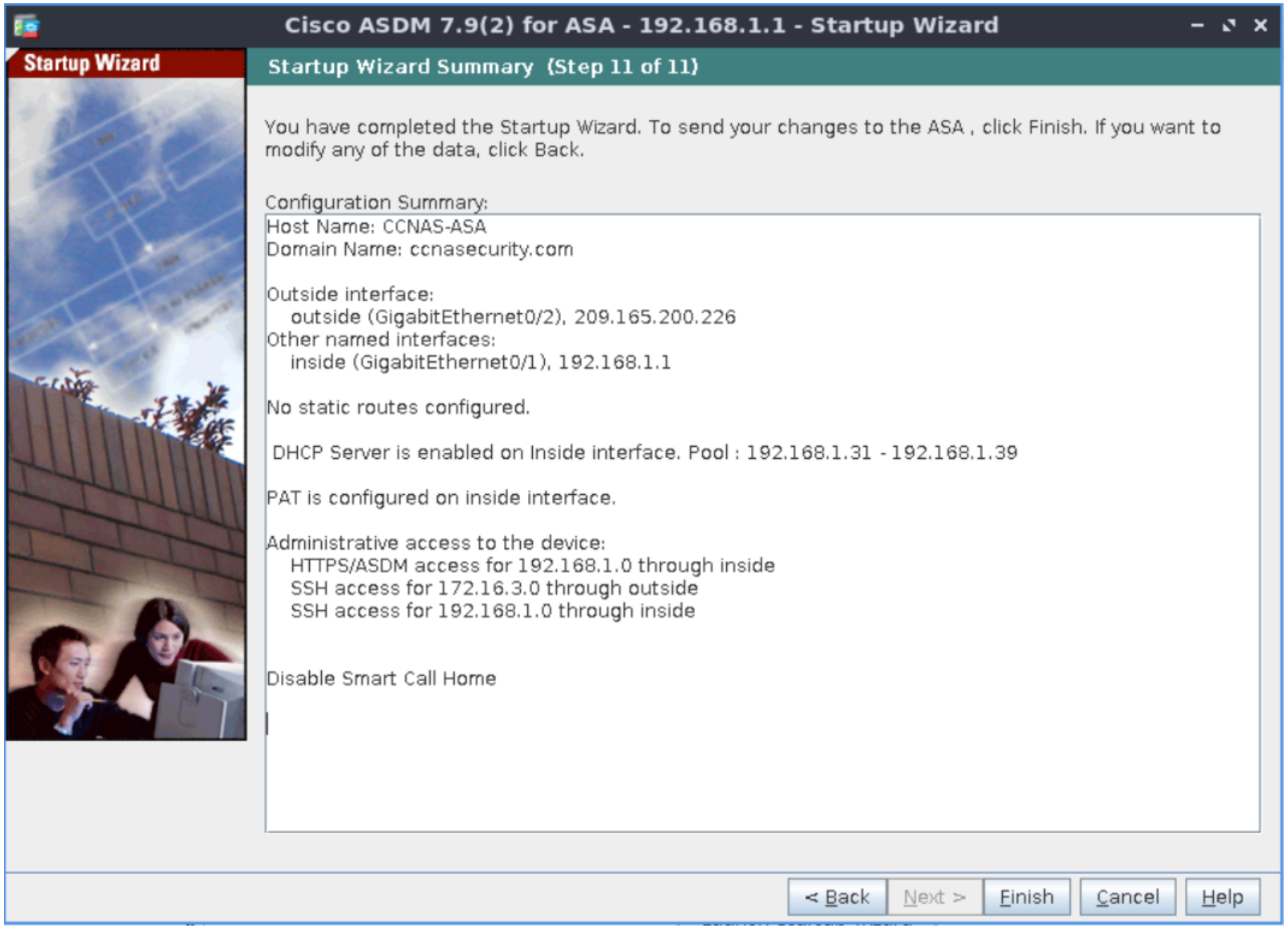

Cisco ASDM 7.9(2) for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
DHCP Server (Step 6 of 11)
The ASA can act as a DHCP server and provide IP addresses to the hosts on your Inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.
Enable DHCP server on the inside interface
DHCP Address Pool
Starting IP Address: 192.168.1.31
Ending IP Address: 192.168.1.39
DHCP Parameters
DNS Server 1: 10.20.30.40
DNS Server 2:
WINS Server 1:
WINS Server 2:
Lease Length:
sec
Ping Timeout:
ms
Domain Name: ccnasecurity.com
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.
Enable auto-configuration from interface:
outside
< Back
Next >
Finish
Cancel
Help

Port Address Translation (PAT)

SSH


Cisco ASDM 7.9(2) for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Administrative Access (Step 8 of 11)
Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.
Type
Interface
IP Address
Mask/ Prefix Length
HTTPS/ASDM
inside
192.168.1.0
255.255.255.0
SSH
inside
192.168.1.0
255.255.255.0
SSH
outside
172.16.3.0
255.255.255.0
Add
Edit
Delete
Enable HTTP server for HTTPS/ASDM access
Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.
Enable ASDM history metrics
< Back
Next >
Finish
Cancel
Help

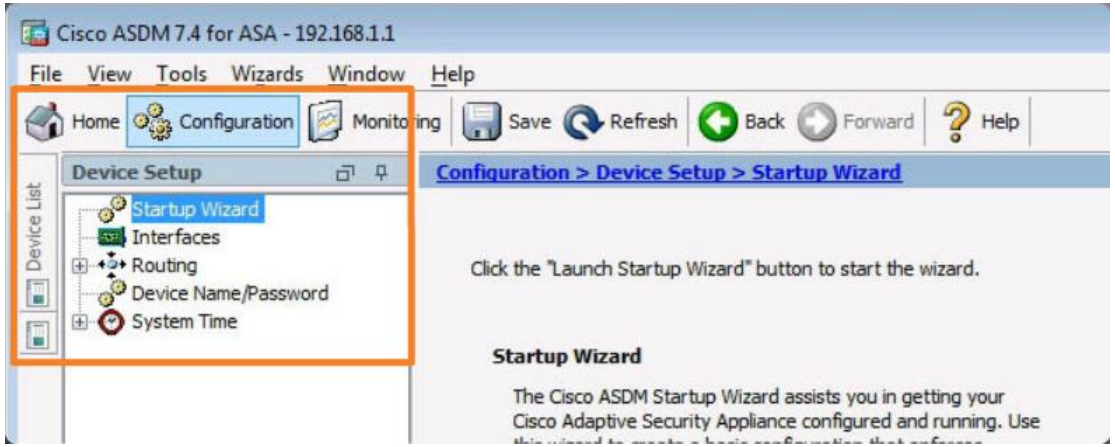
Kontrola konfigurácie



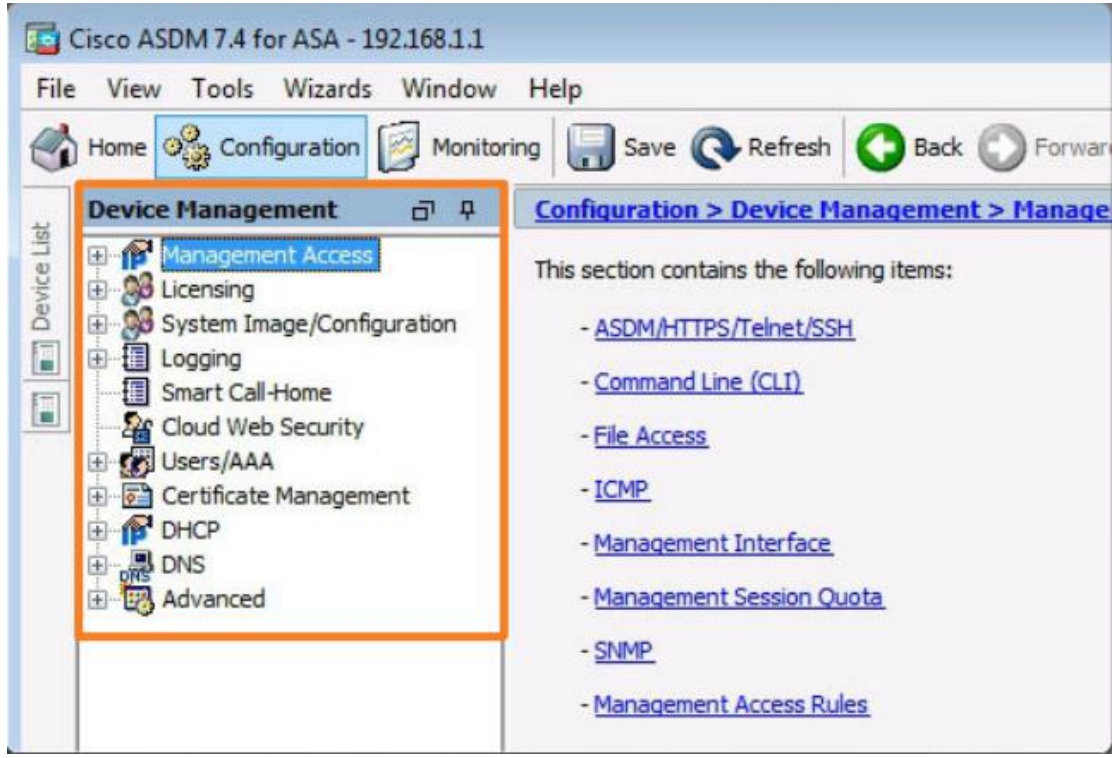
Základná konfigurácia cez ASDM

ASDM – základné nastavenia

Položka Nastavenie zariadenia

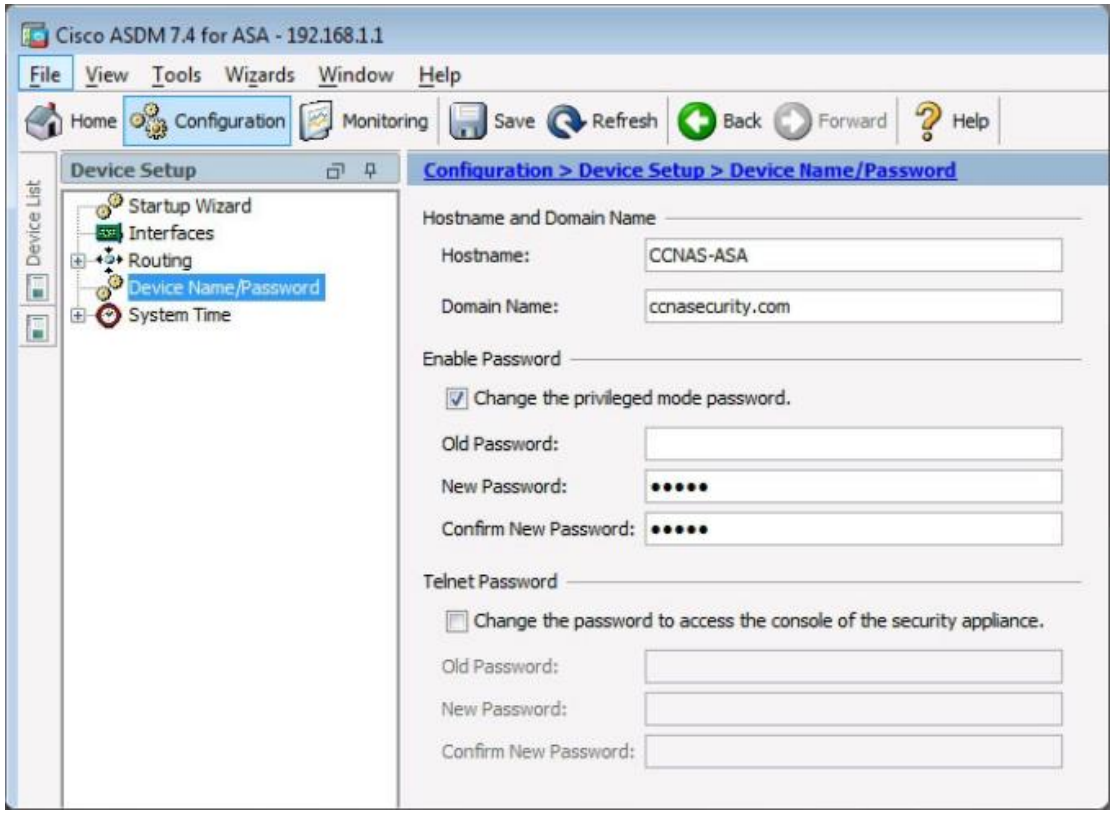


Položka Manažment zariadenia

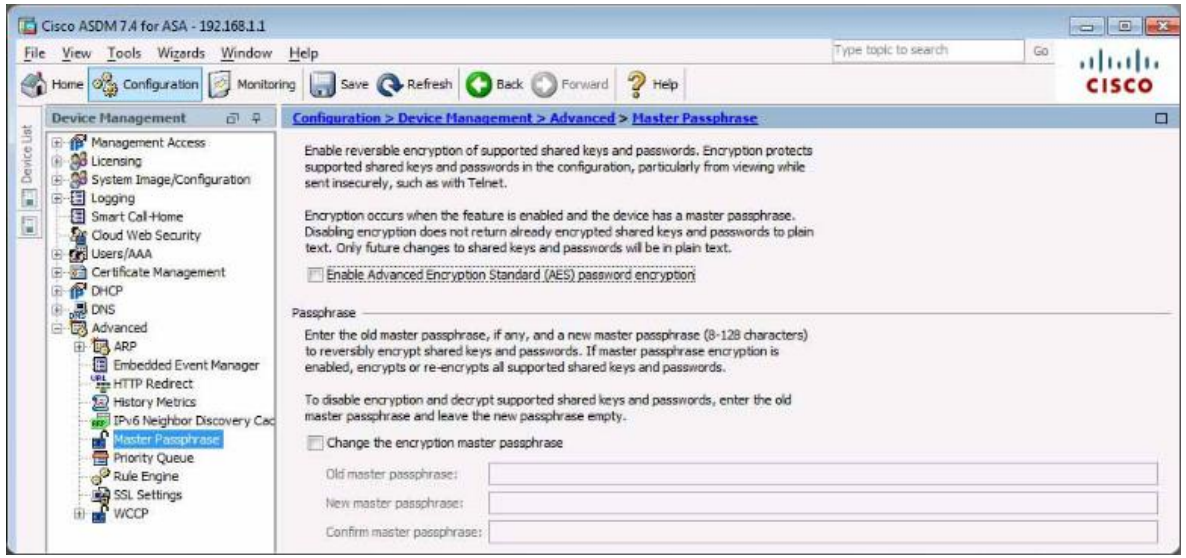


ASDM – základné nastavenia

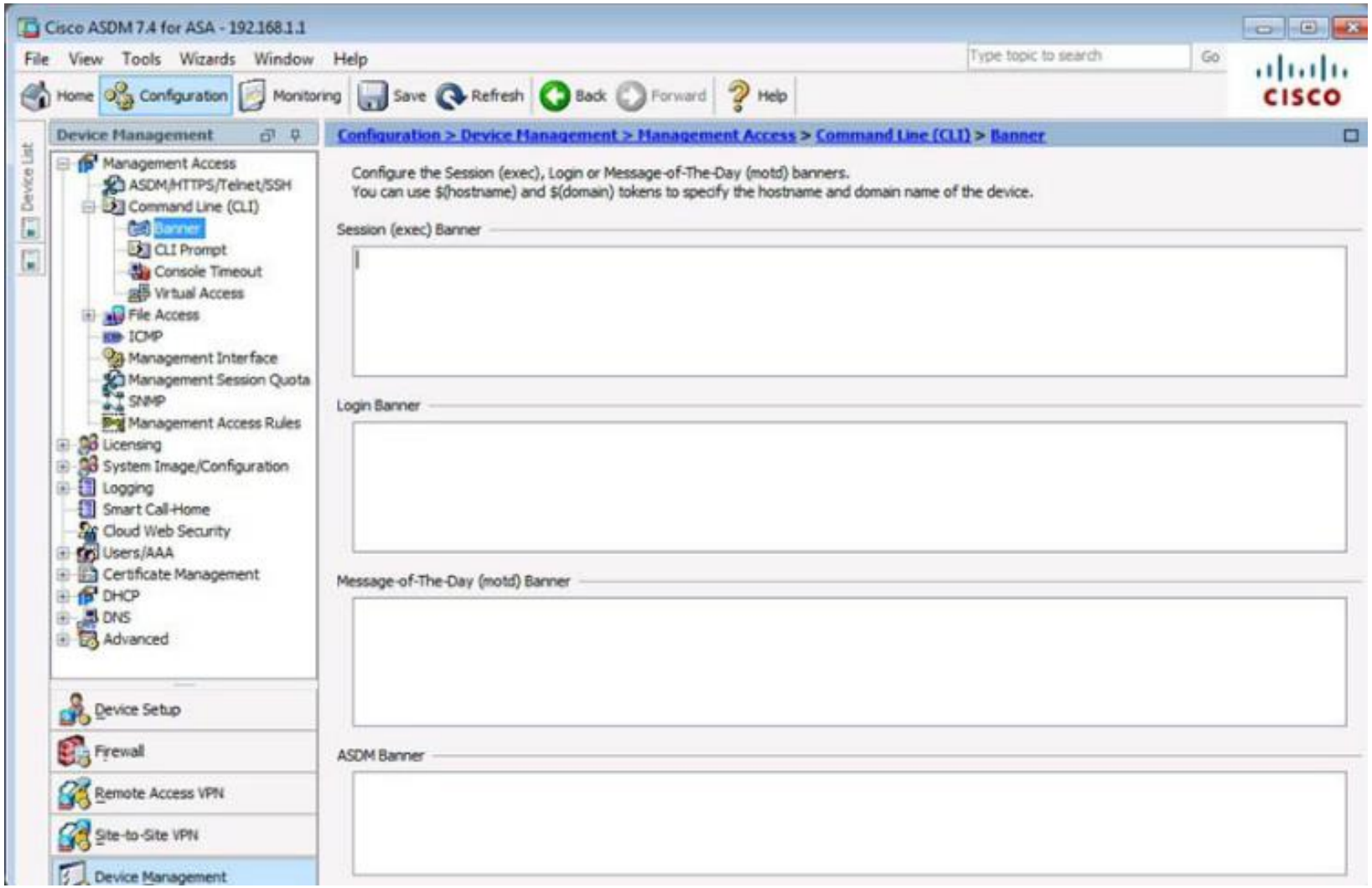
Configuring Hostname, Domain Name, and Enable Password



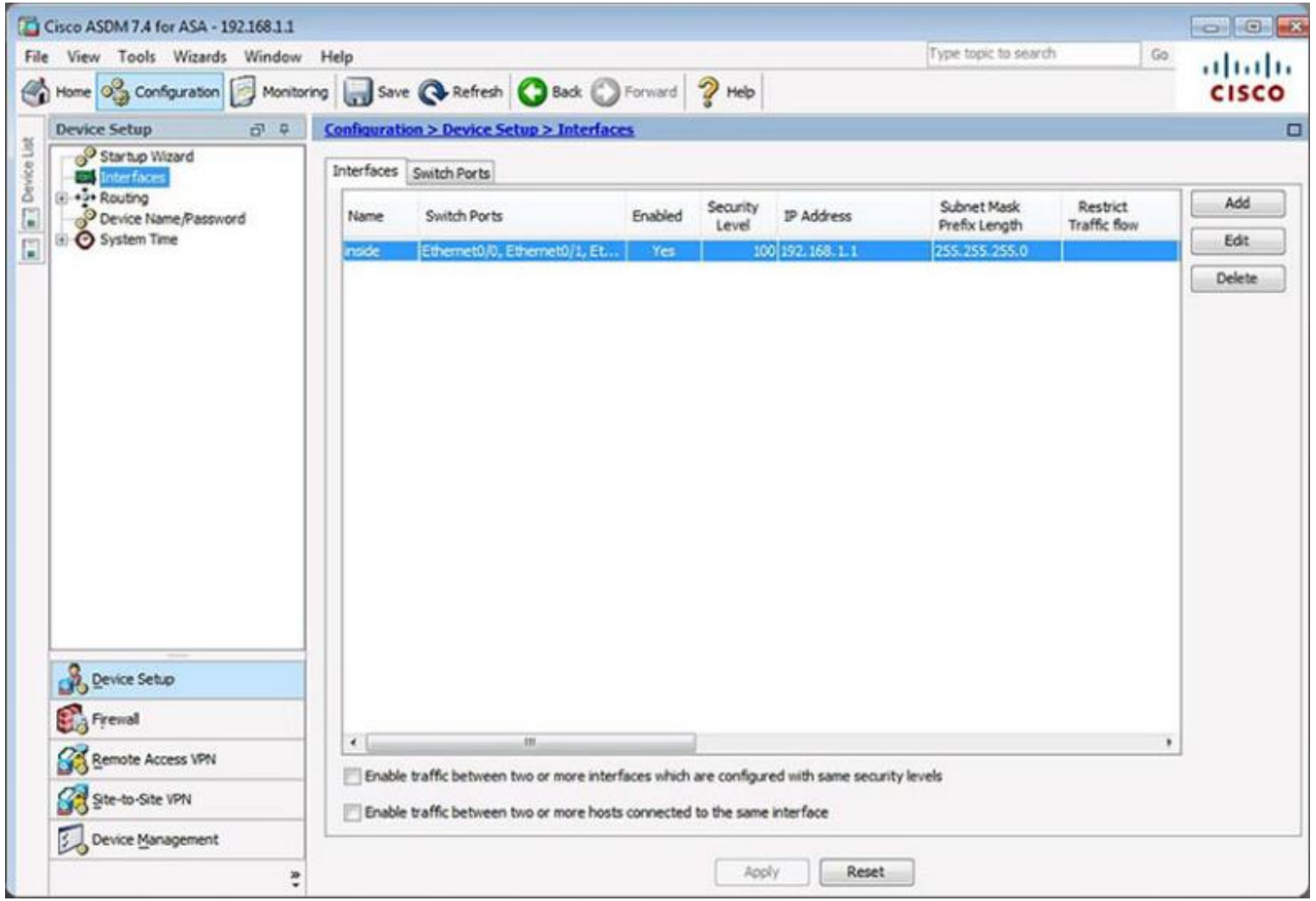
Configuring a Master Passphrase



ASDM – základné nastavenia - bannery

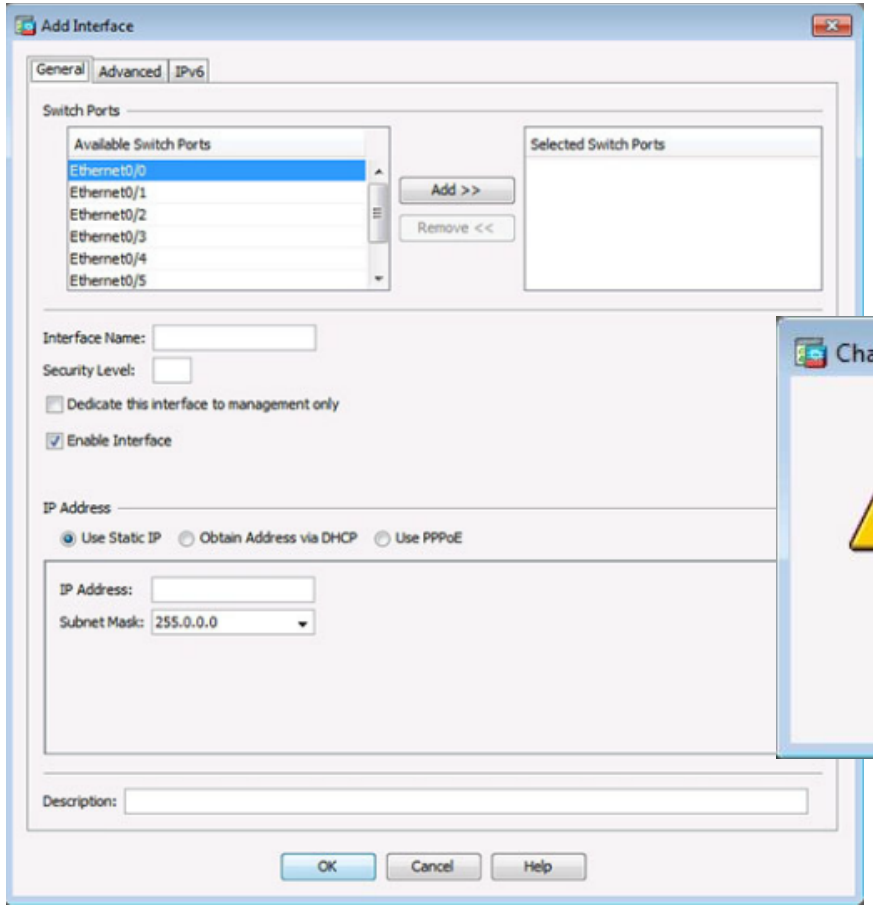


Konfigurácia rozhraní

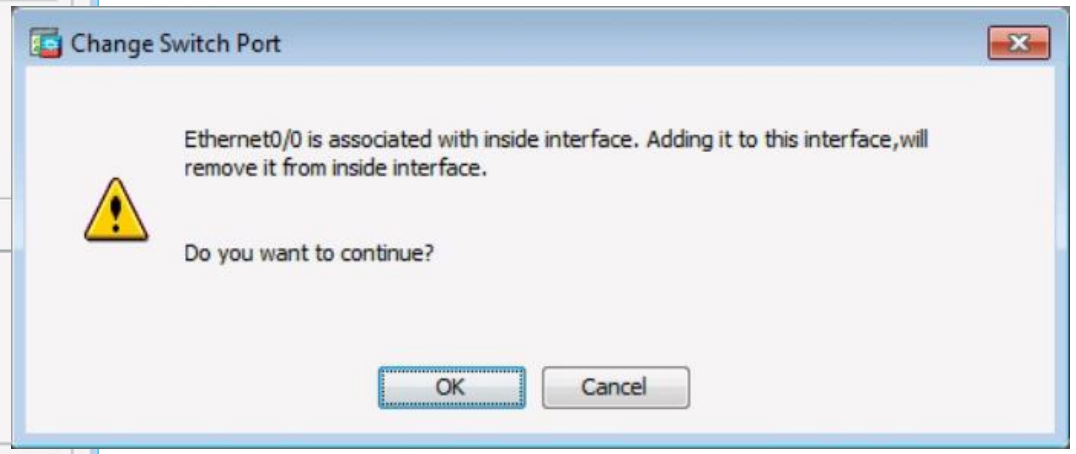


Konfigurácia rozhraní

Adding an Outside Interface

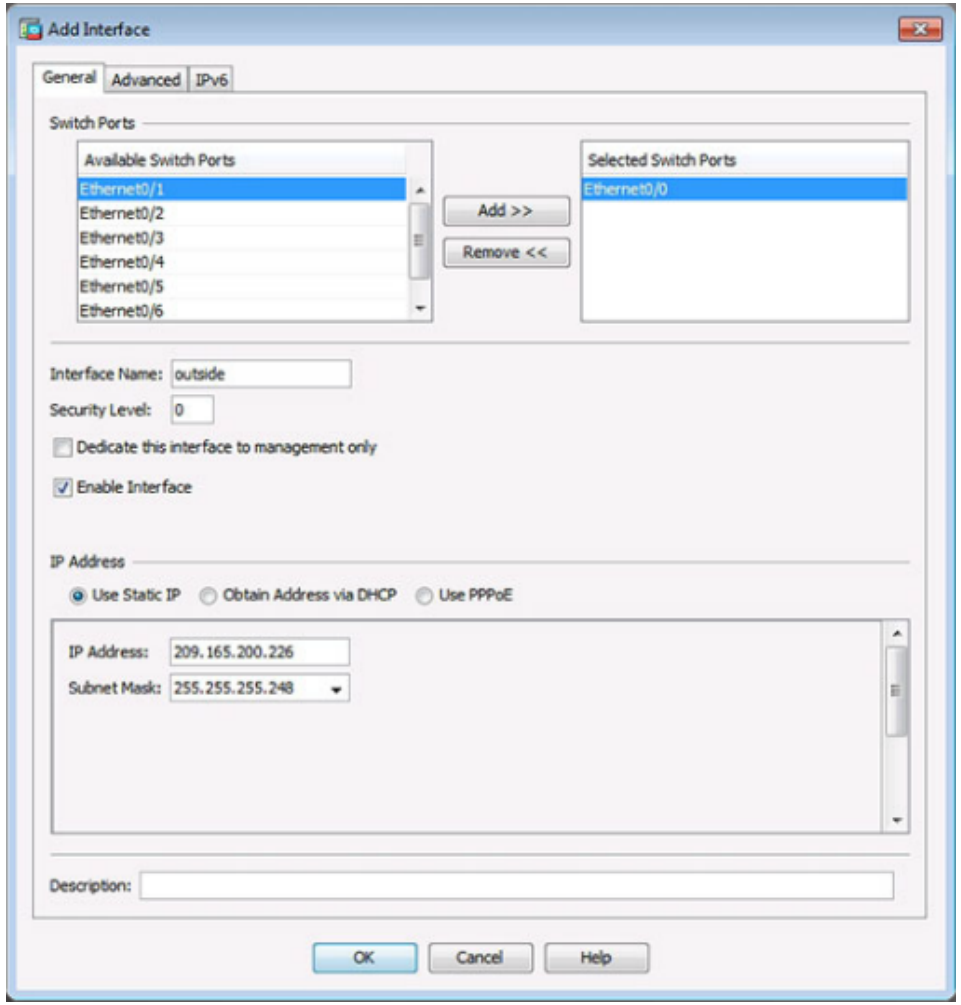


Change Switch Port Window

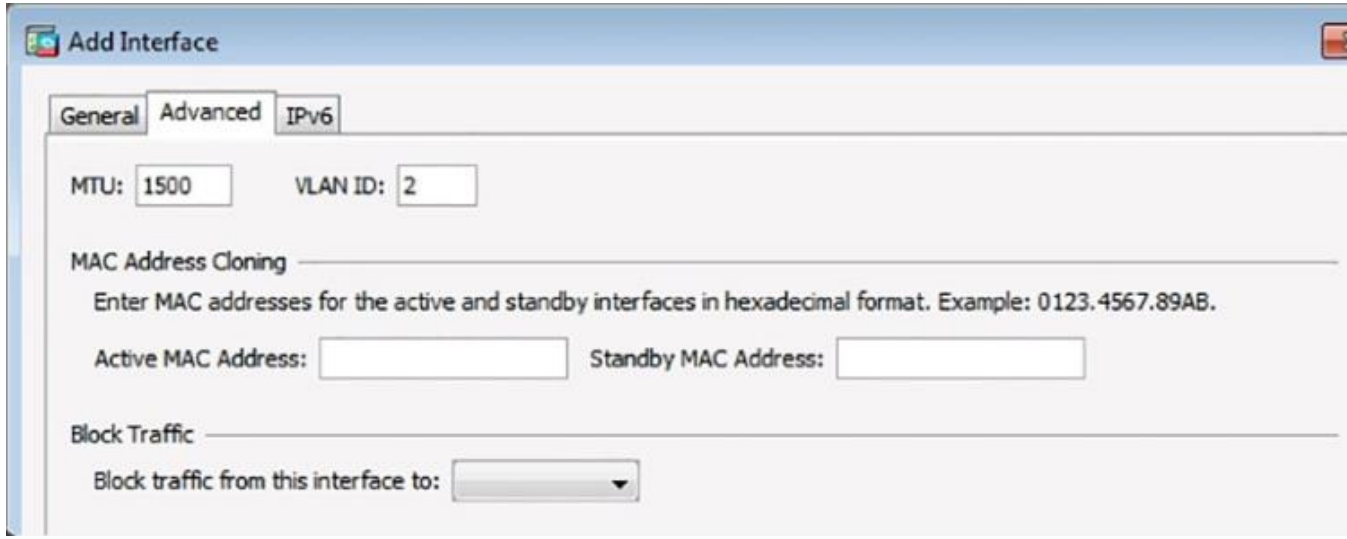


Konfigurácia rozhraní

Adding an Outside Interface



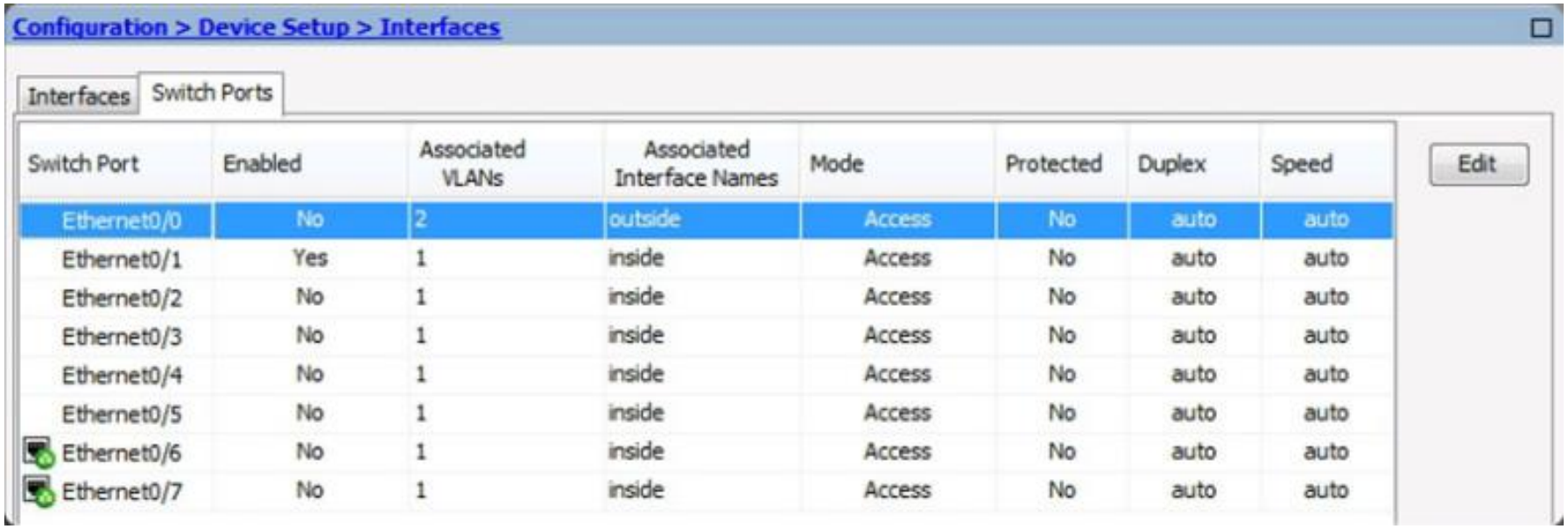
Advanced Outside Interface Settings



Updated Interface Page

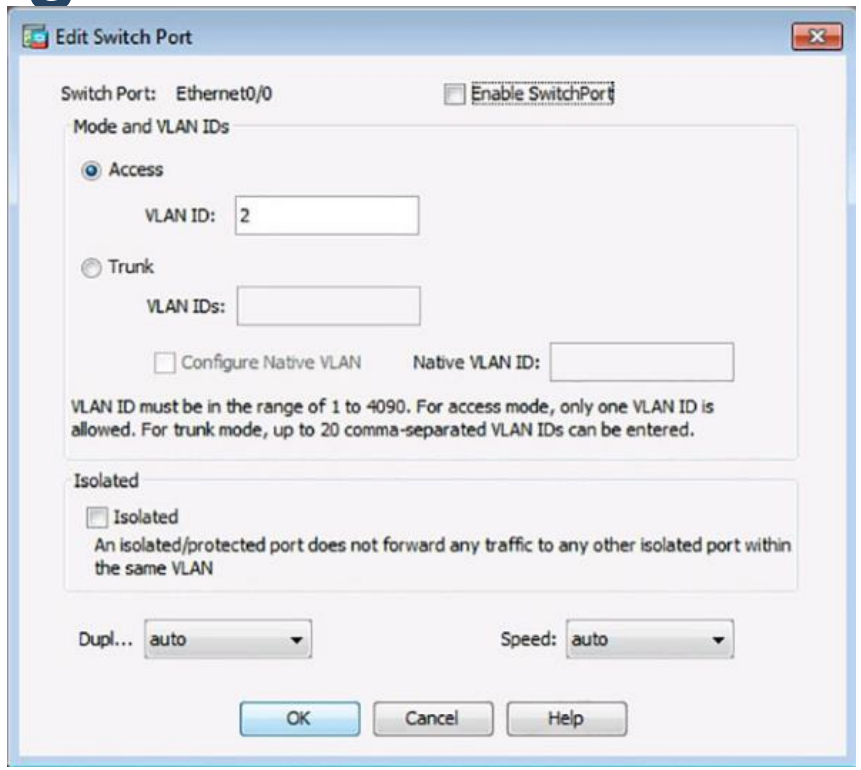
Konfigurácia rozhraní

Verifying Interfaces



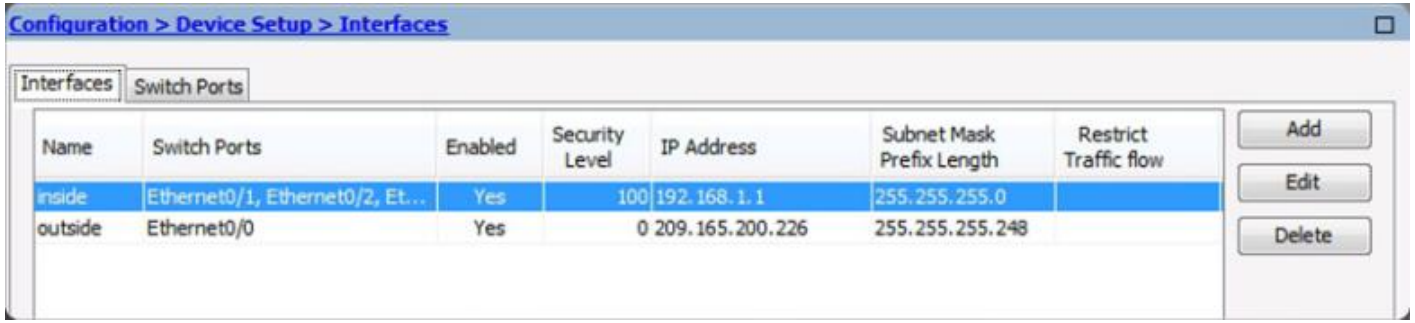
Switch Port	Enabled	Associated VLANs	Associated Interface Names	Mode	Protected	Duplex	Speed
Ethernet0/0	No	2	outside	Access	No	auto	auto
Ethernet0/1	Yes	1	inside	Access	No	auto	auto
Ethernet0/2	No	1	inside	Access	No	auto	auto
Ethernet0/3	No	1	inside	Access	No	auto	auto
Ethernet0/4	No	1	inside	Access	No	auto	auto
Ethernet0/5	No	1	inside	Access	No	auto	auto
Ethernet0/6	No	1	inside	Access	No	auto	auto
Ethernet0/7	No	1	inside	Access	No	auto	auto

Konfigurácia rozhraní

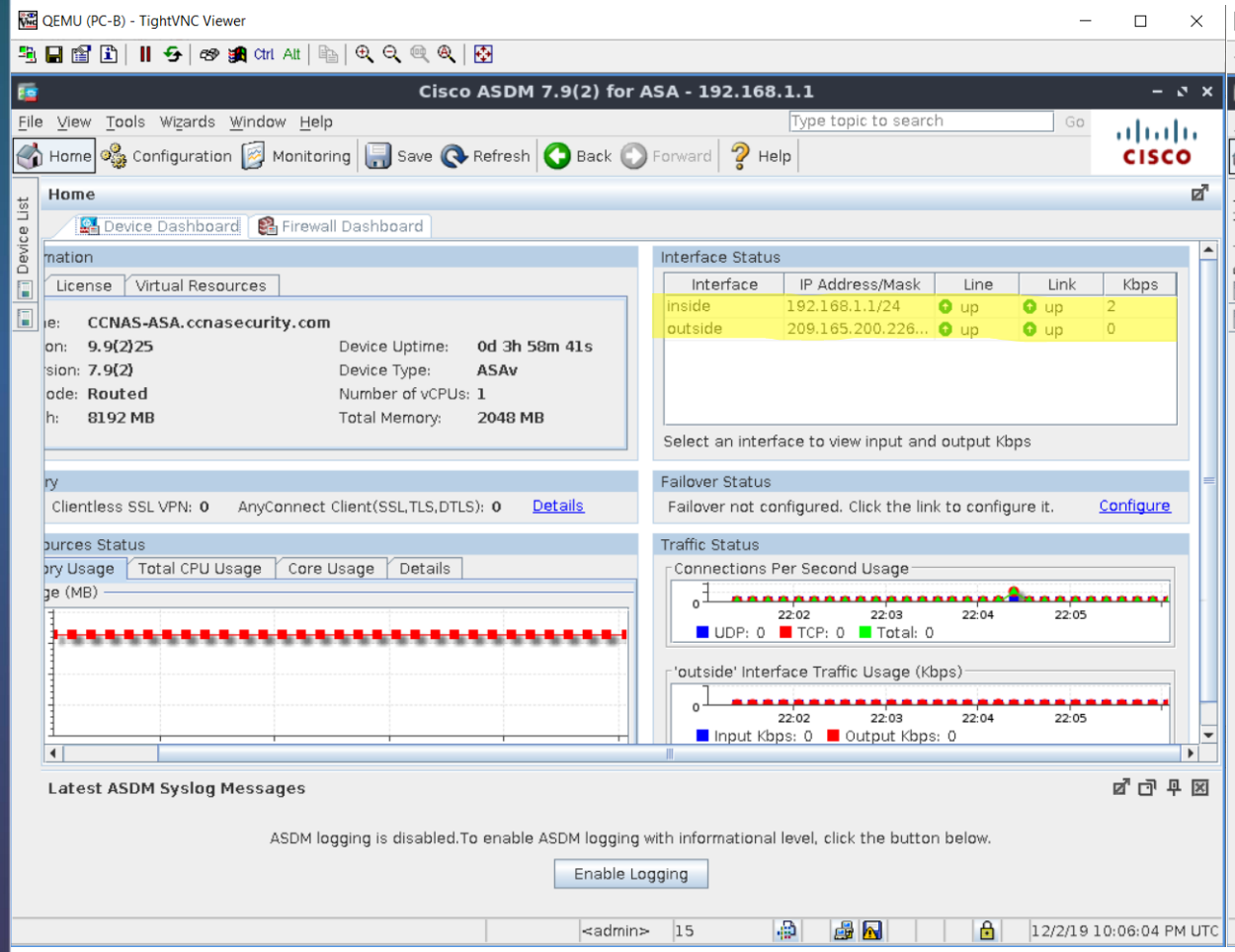


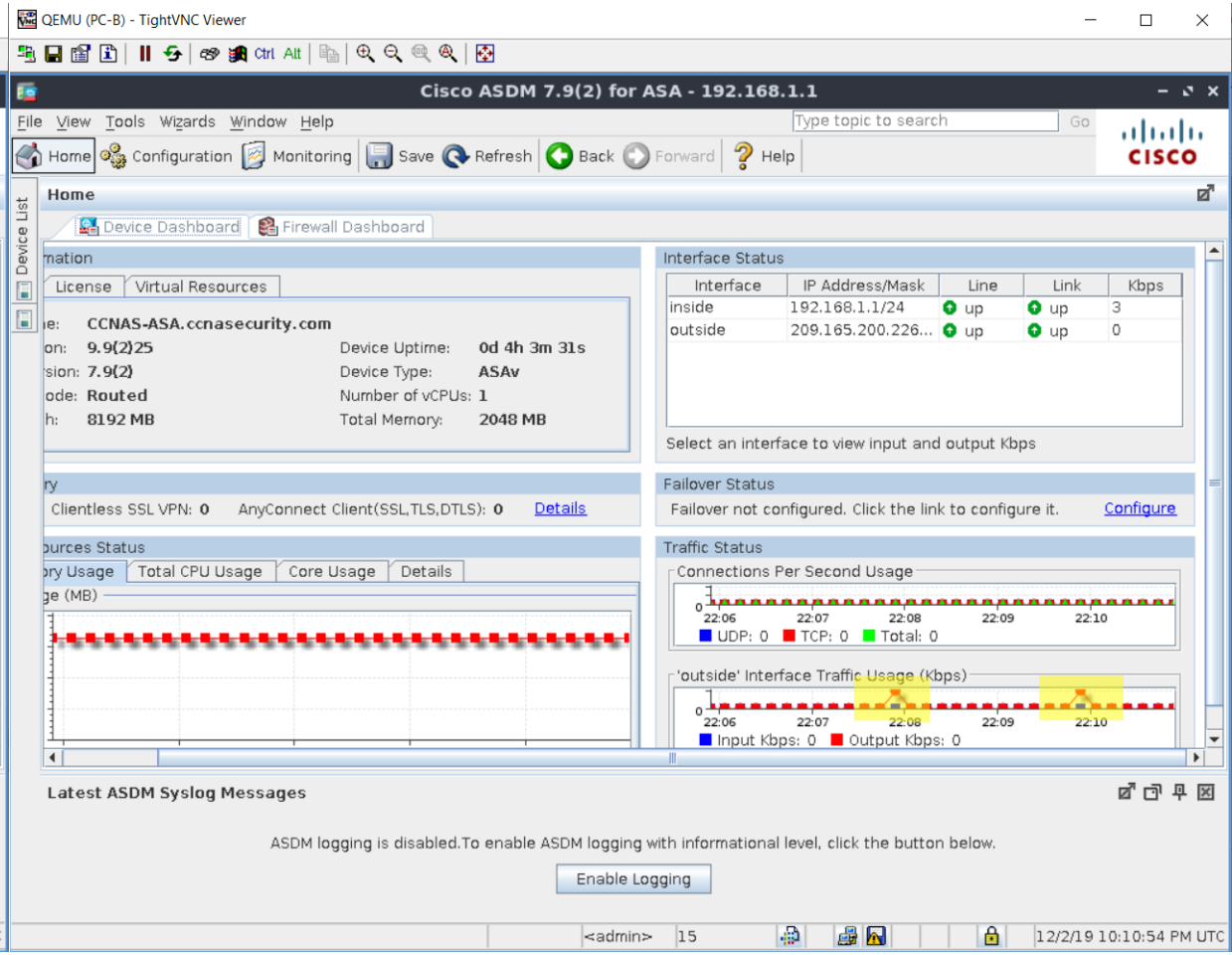
Enable Switch Ports

Apply Configuration

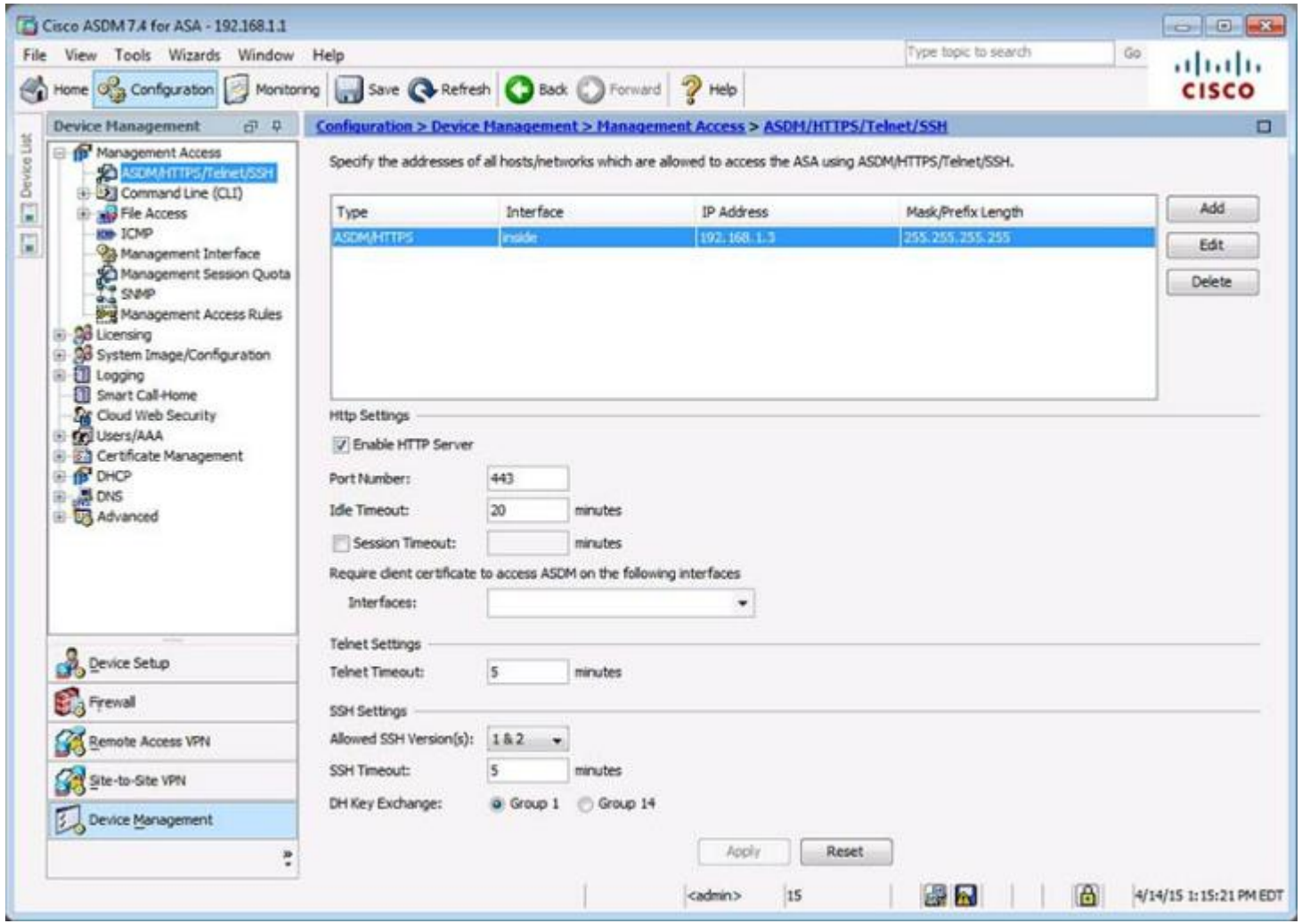


Overenie stavu rozhraní



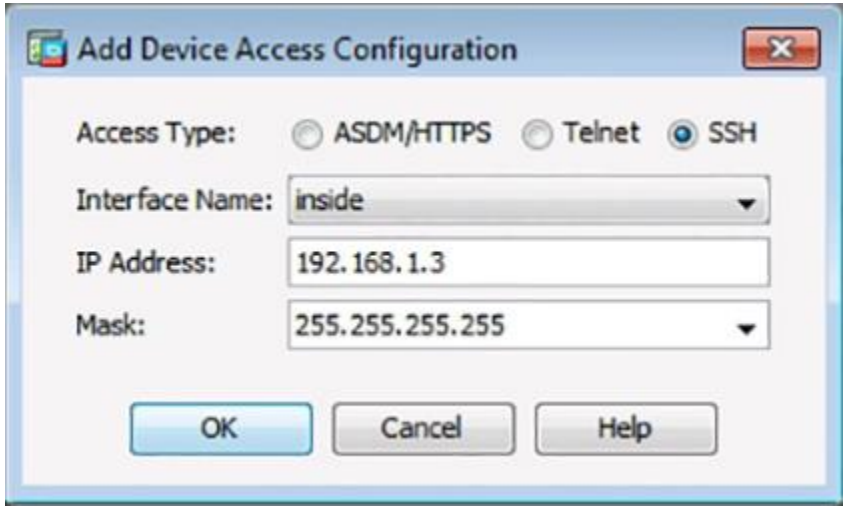


Konfigurácia HTTPS/Telnet/SSH

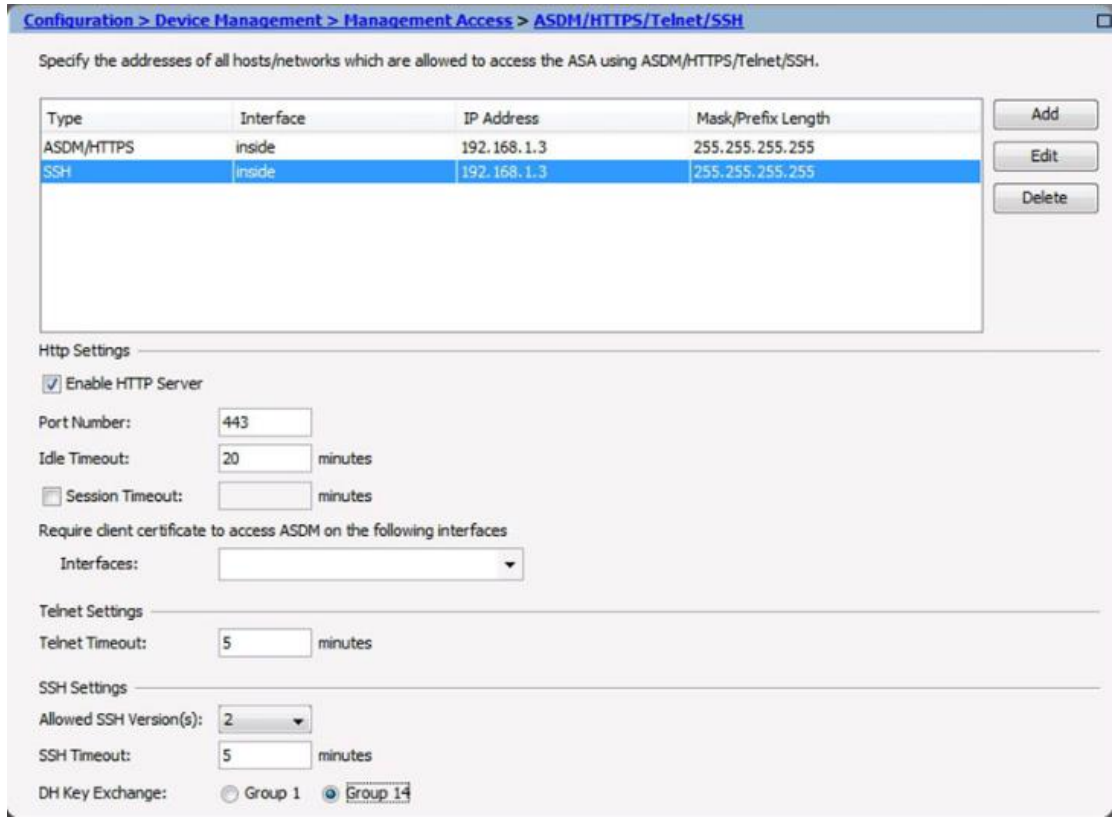


SSH

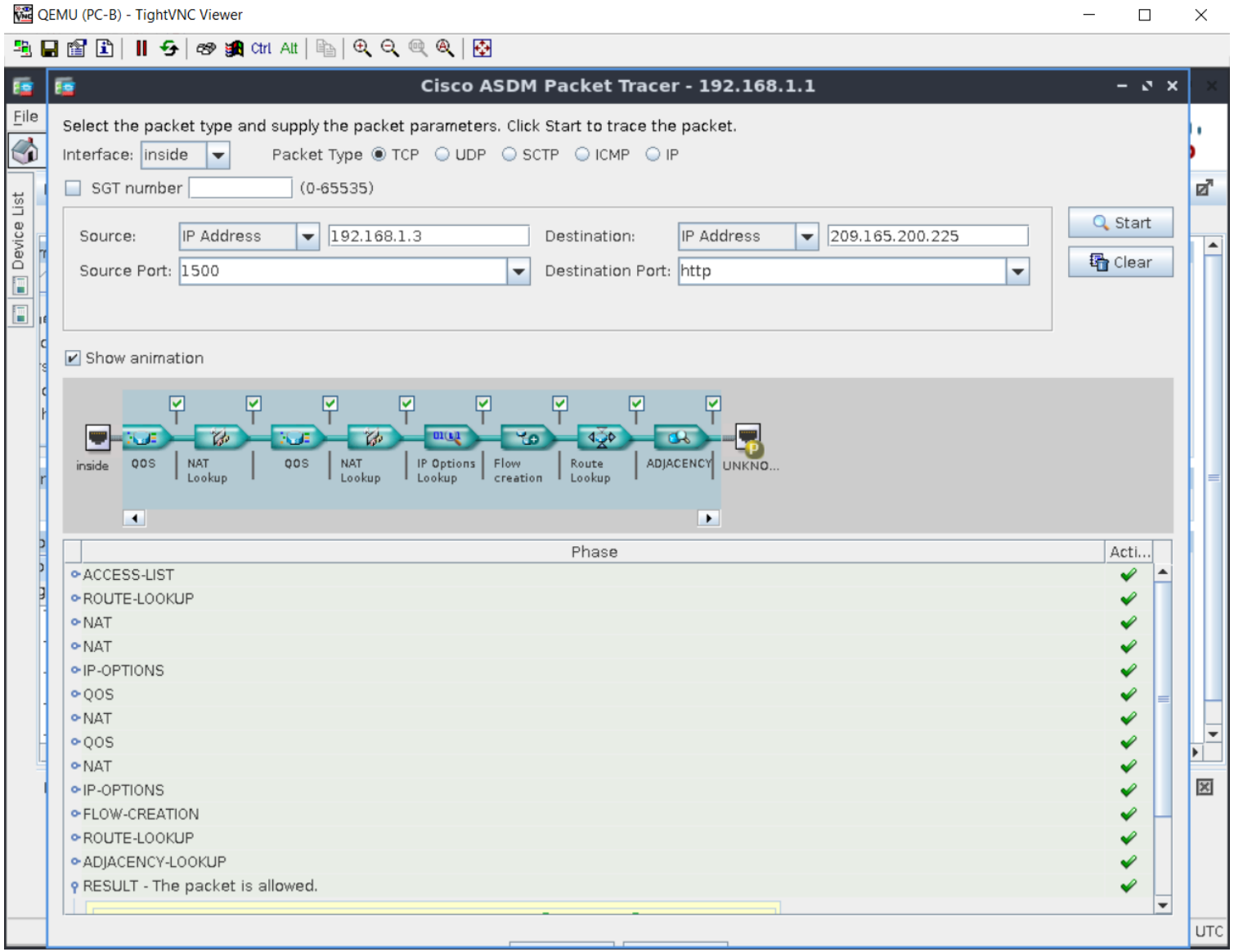
Add Device Access Configuration Window



Configure SSH Settings



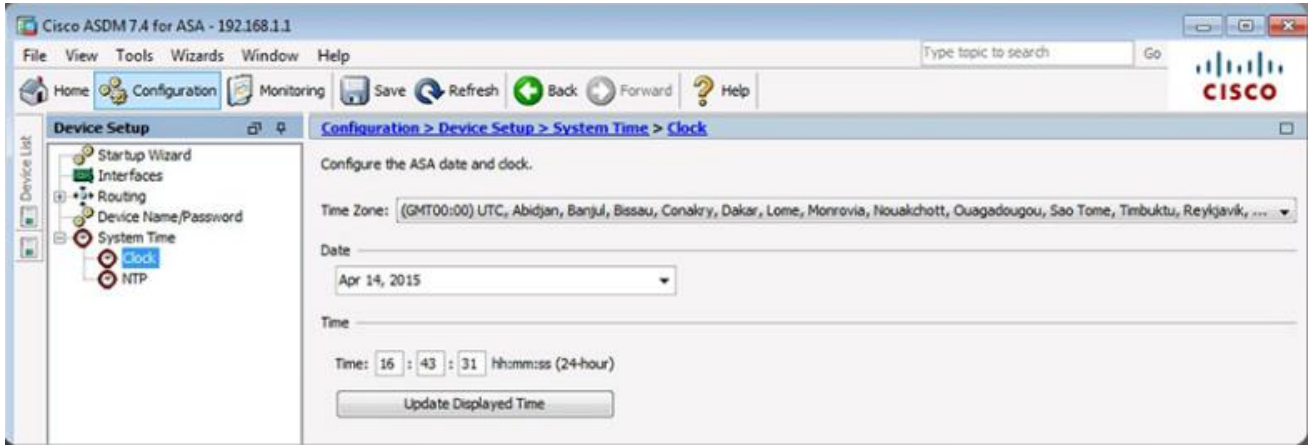
Otestovanie HTTP pripojenia cez Packet Tracer



Konfigurácia ďalších nastavení ASA cez ASDM

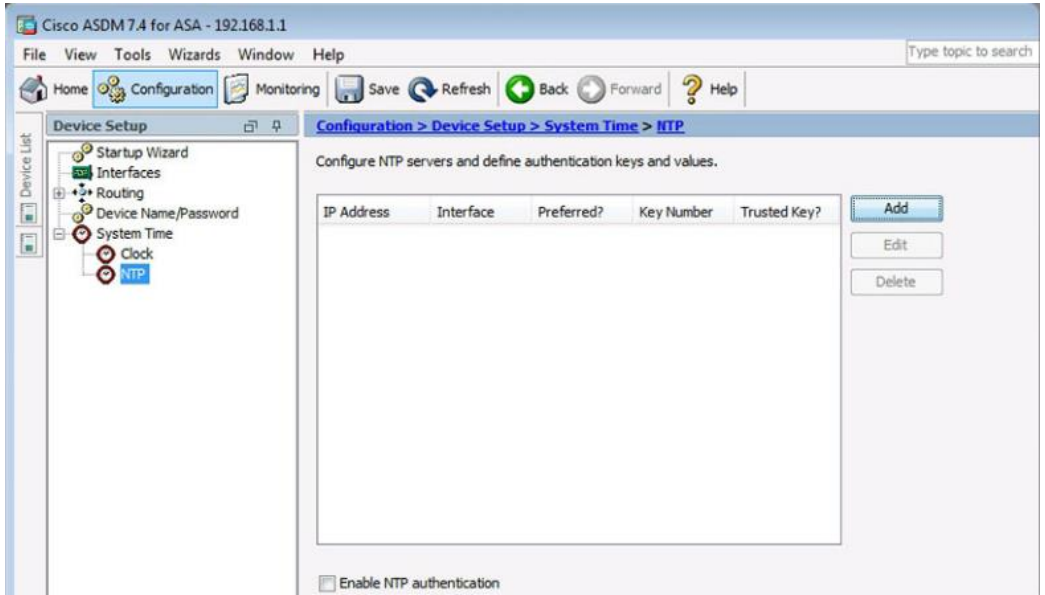
Konfigurácia času

Nastavenie času

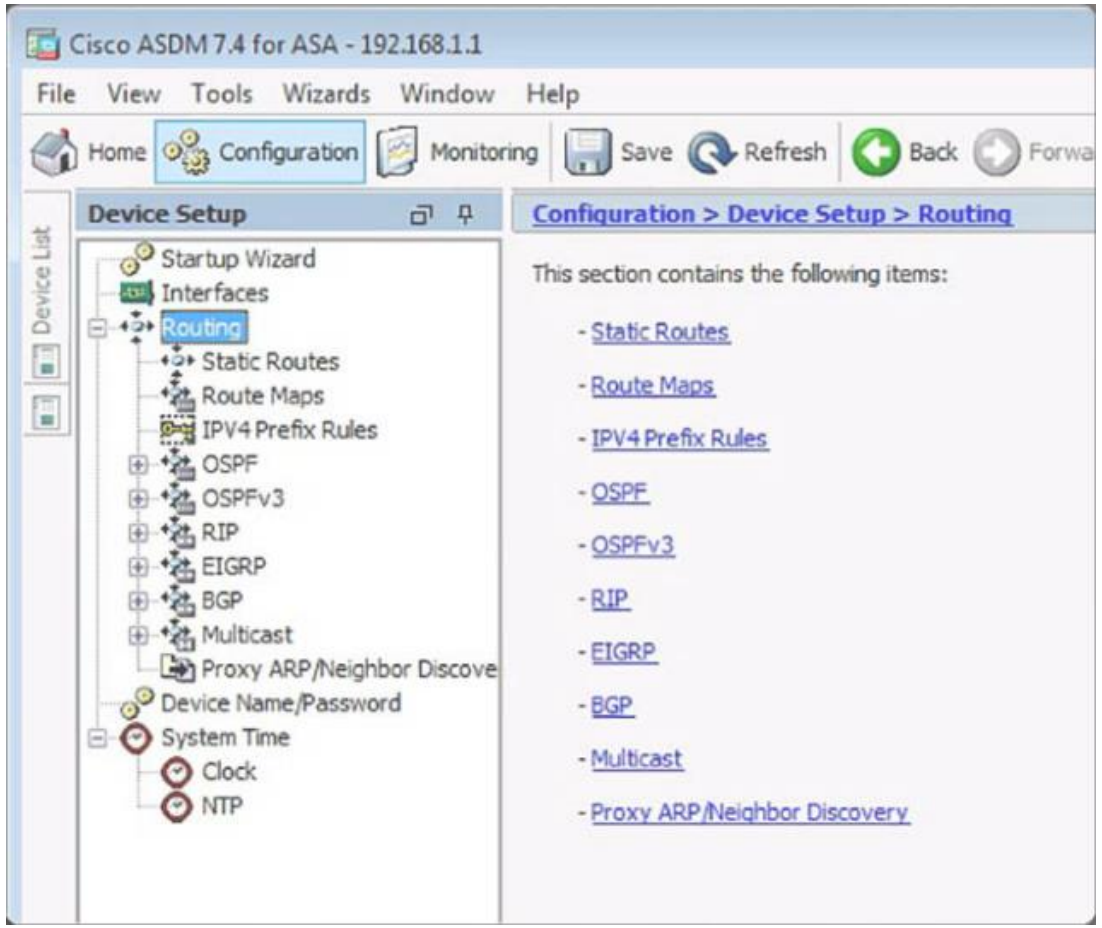


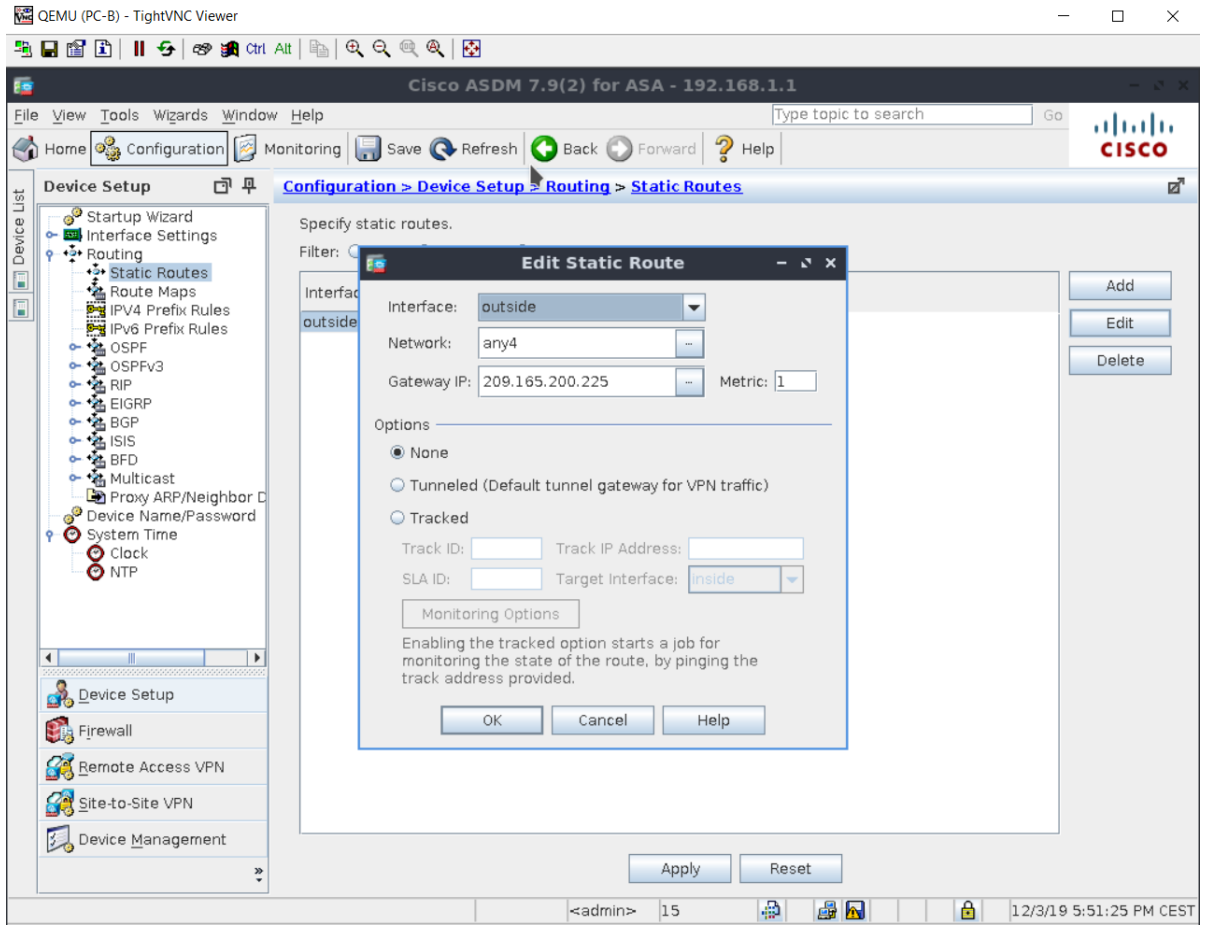
Manually Change the System Time

Use NTP to Change the System Time

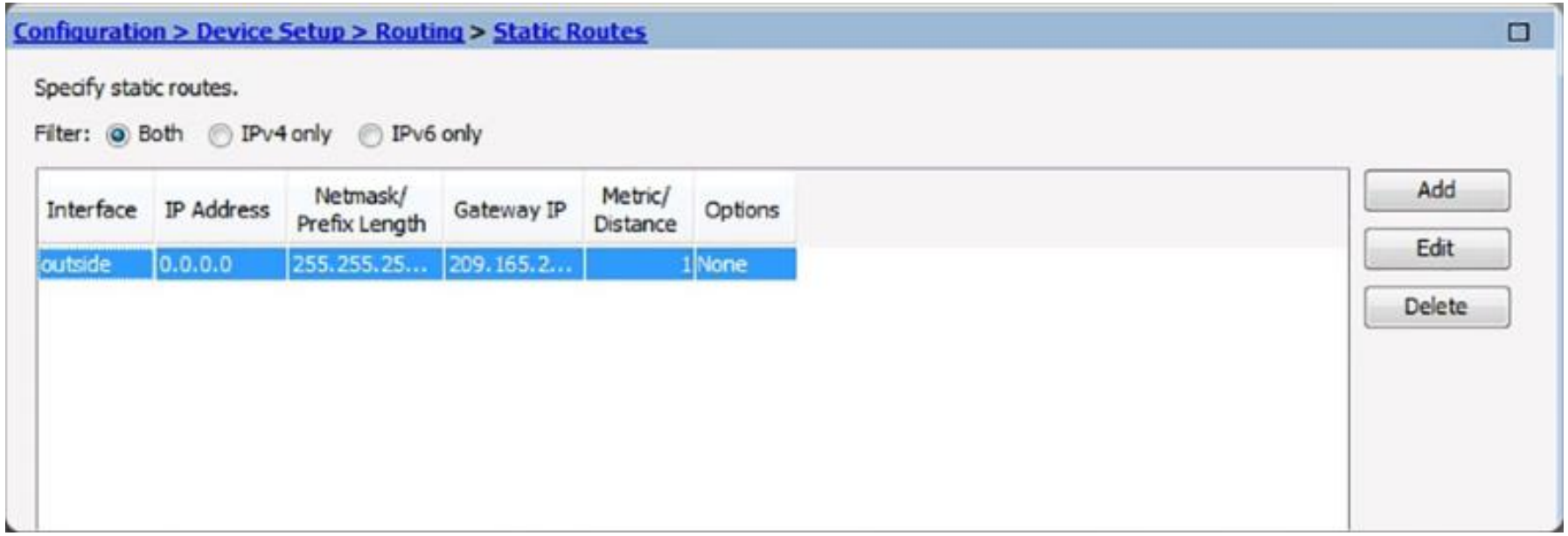


Konfigurácia predvolenej statickej cesty

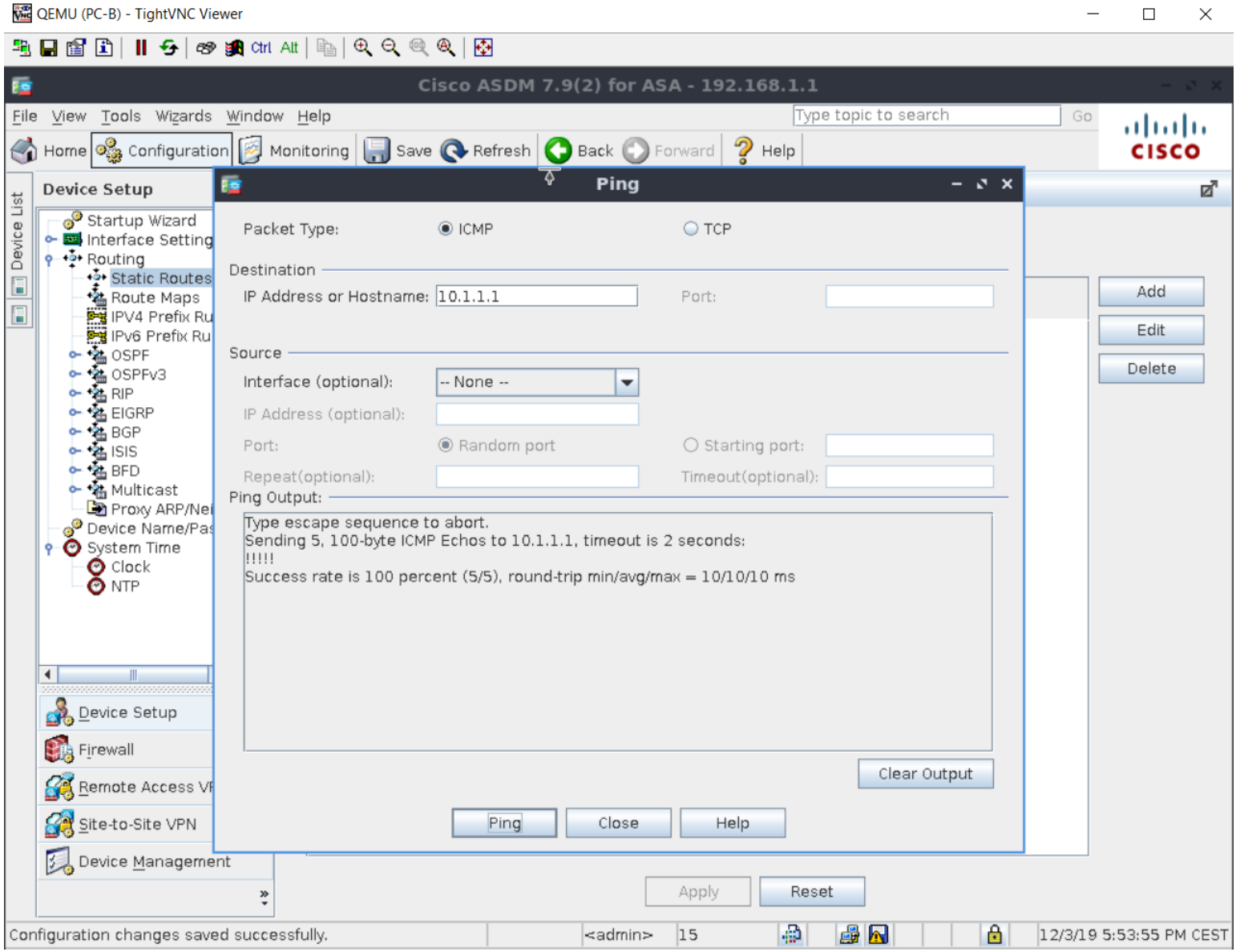




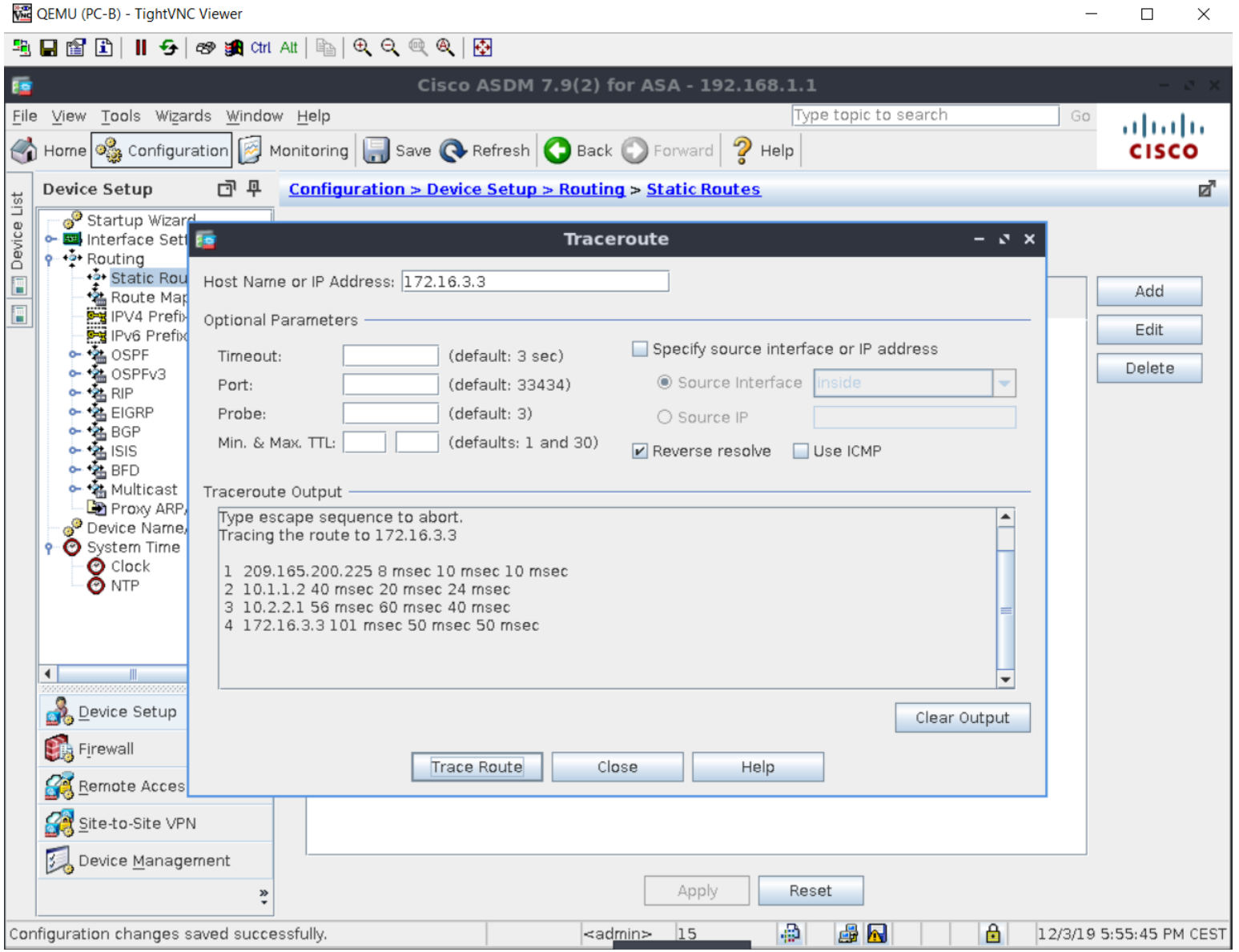
Nezabudni na vždy Apply



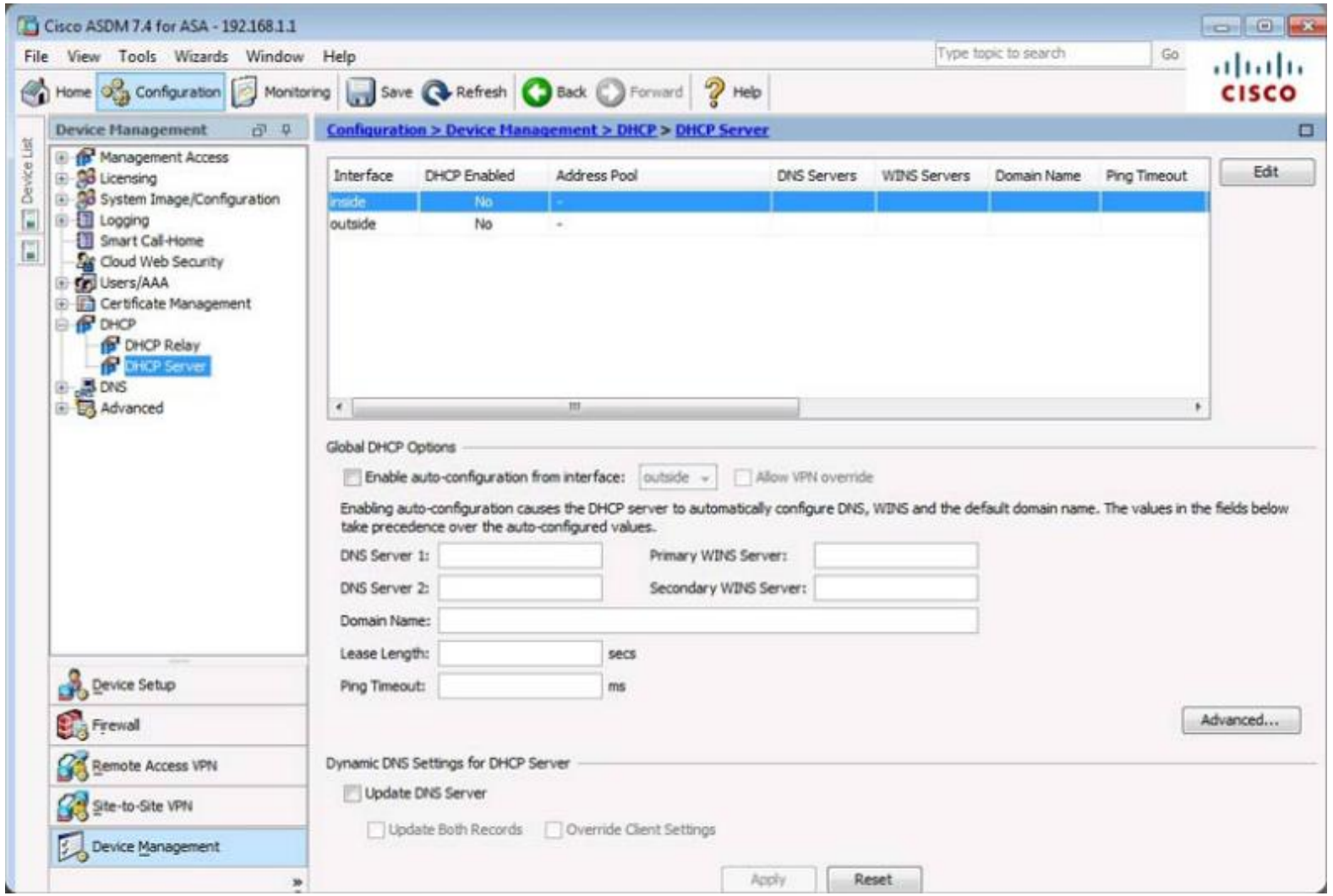
Overenie funkčnosti predvolenej statickej cesty



Traceroute ASA → PC-C

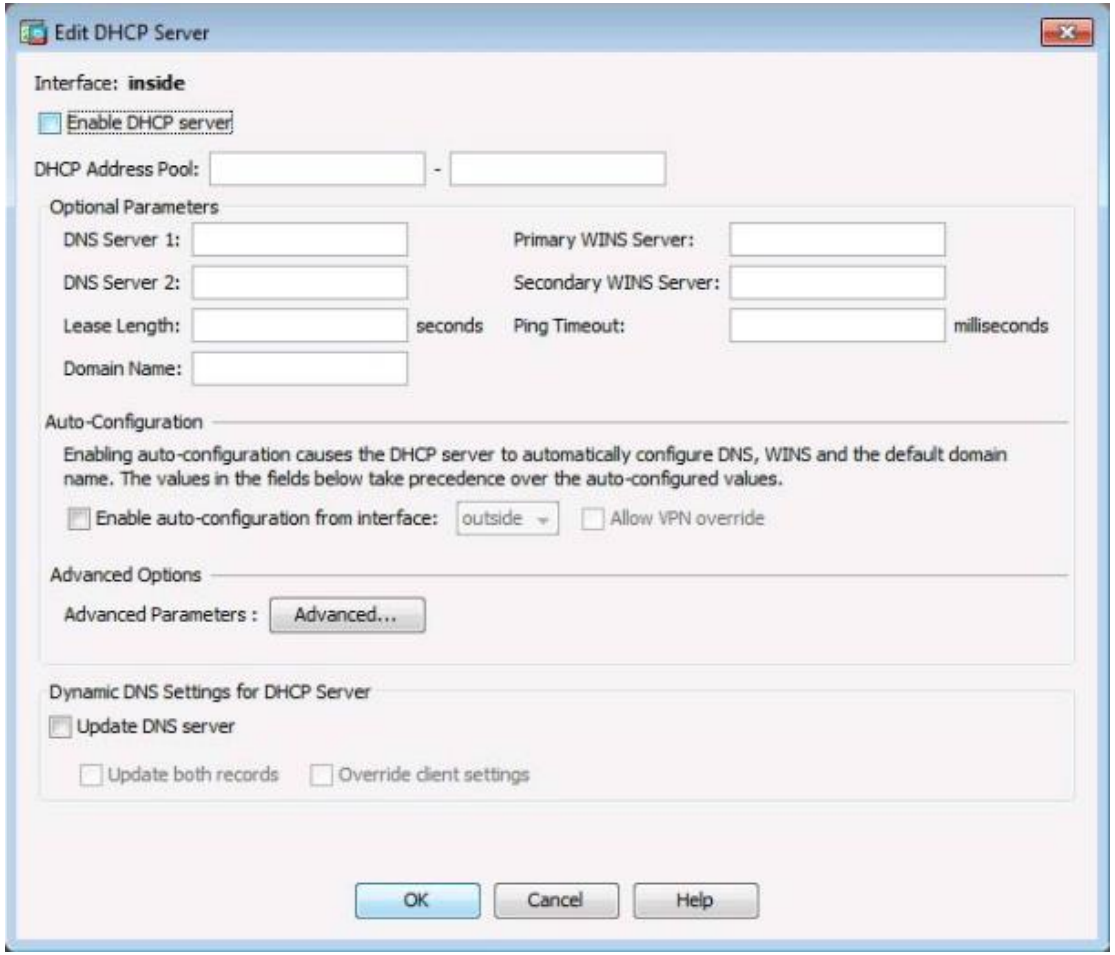


Konfigurácia DHCP služby

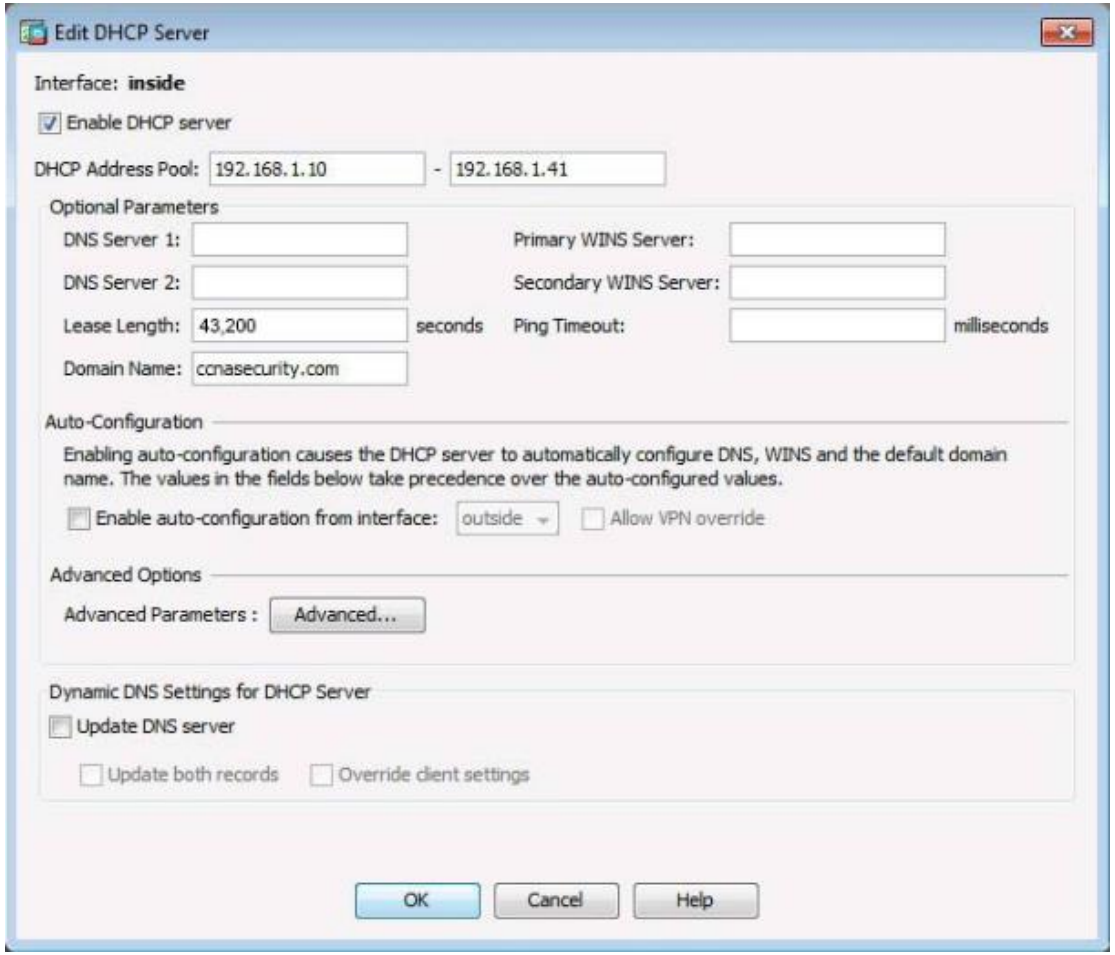


Konfigurácia DHCP služby

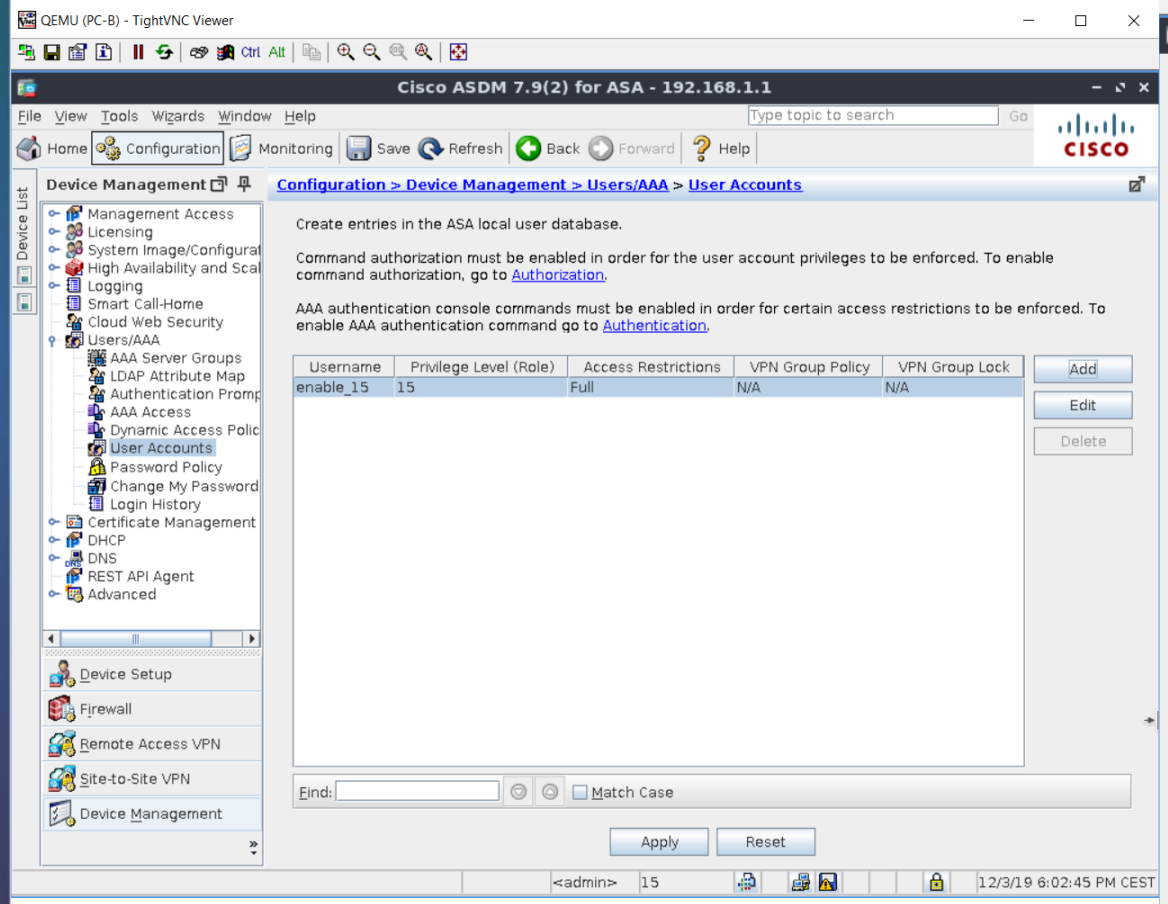
Edit DHCP Server Window

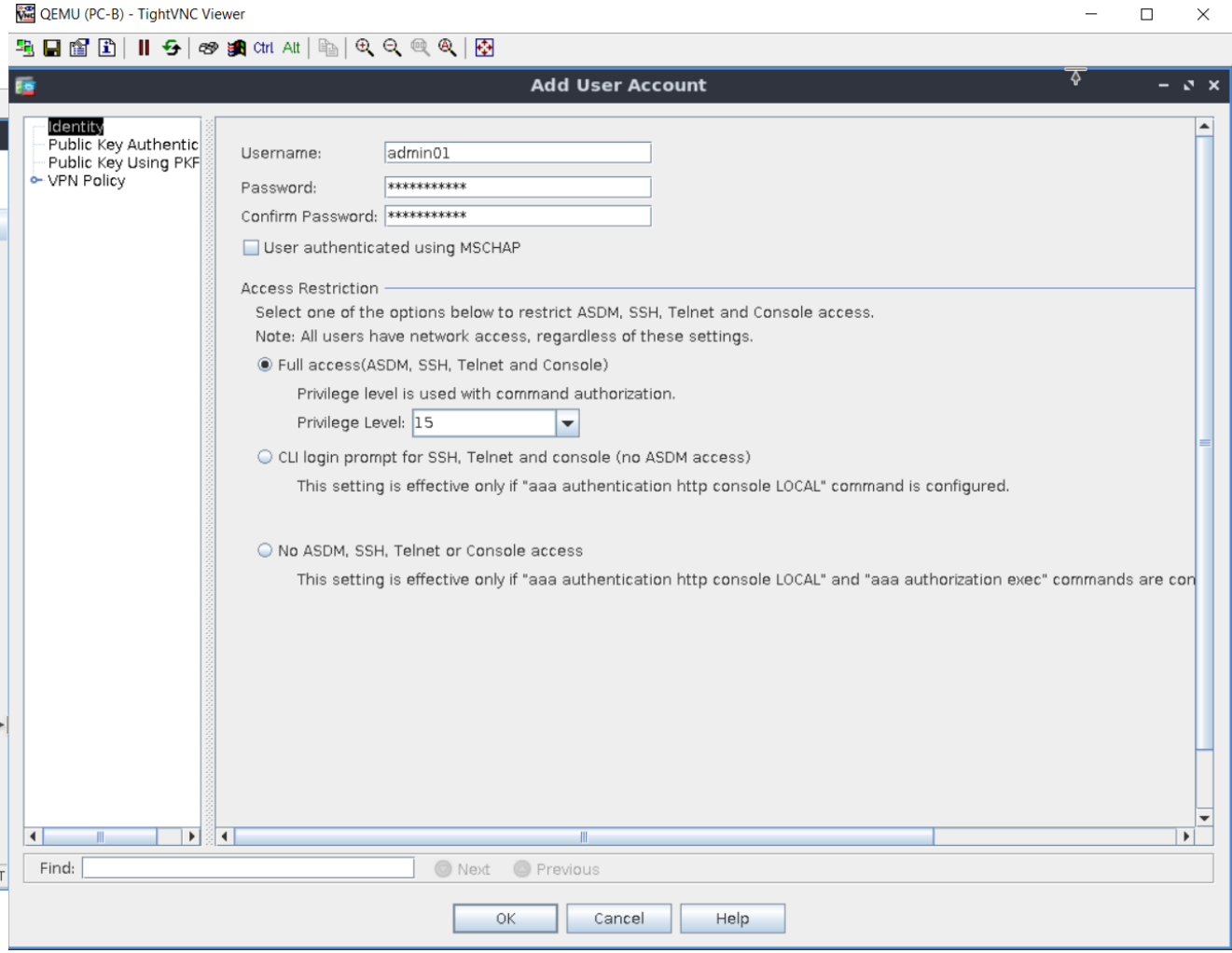


Configuring DHCP Server Services

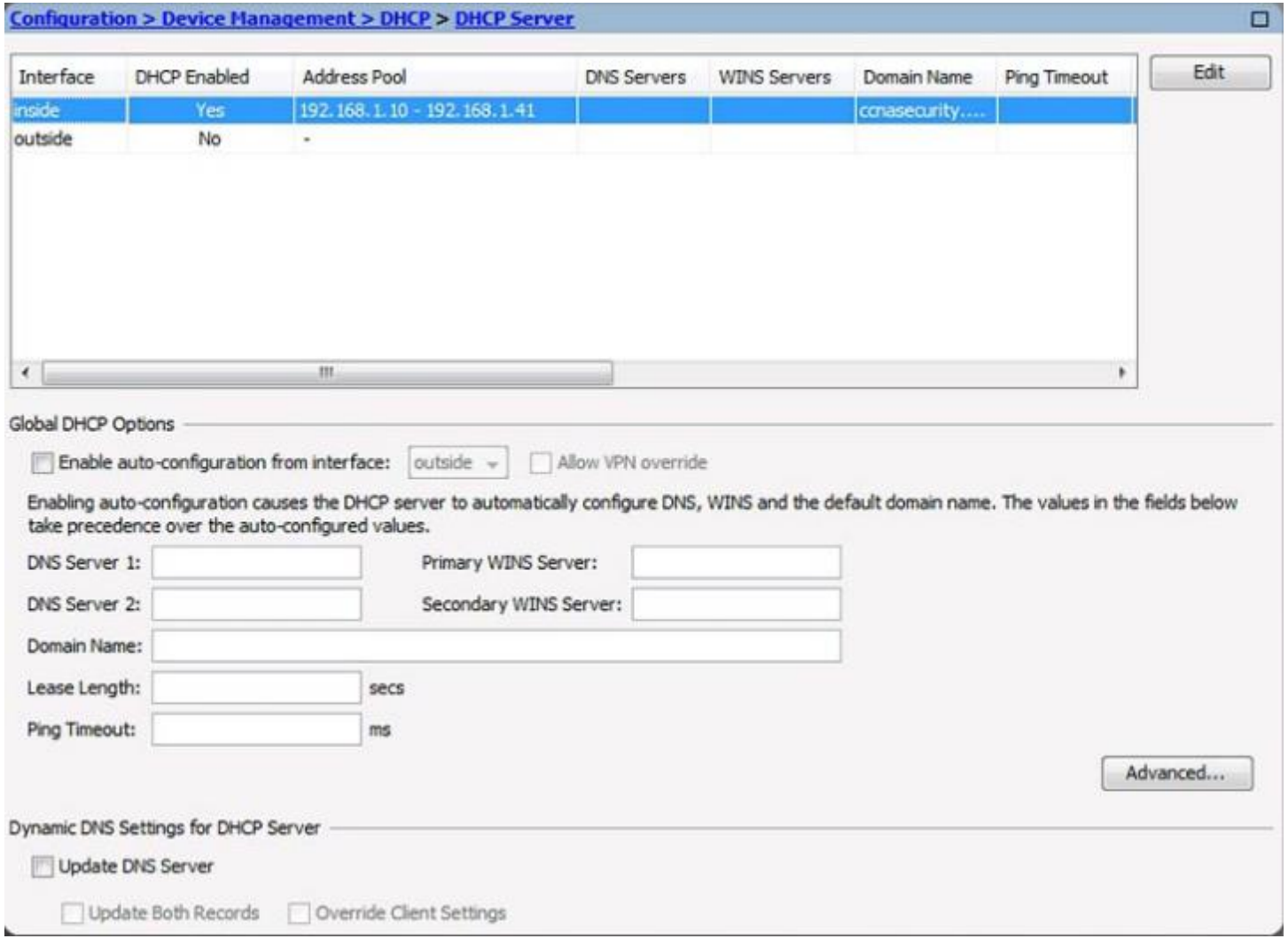


Konfigurácia AAA s využívaním lokálnej DB ASA

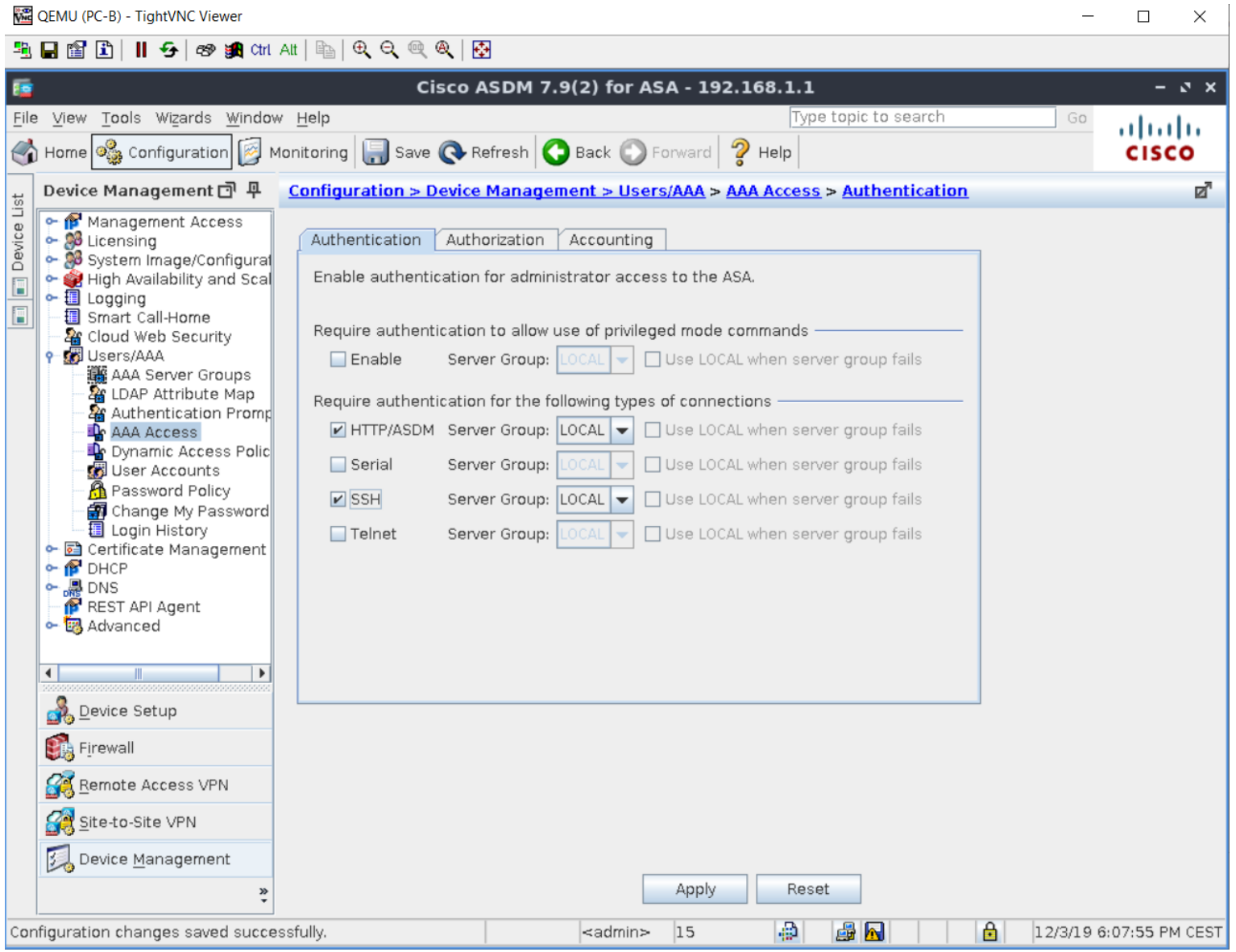




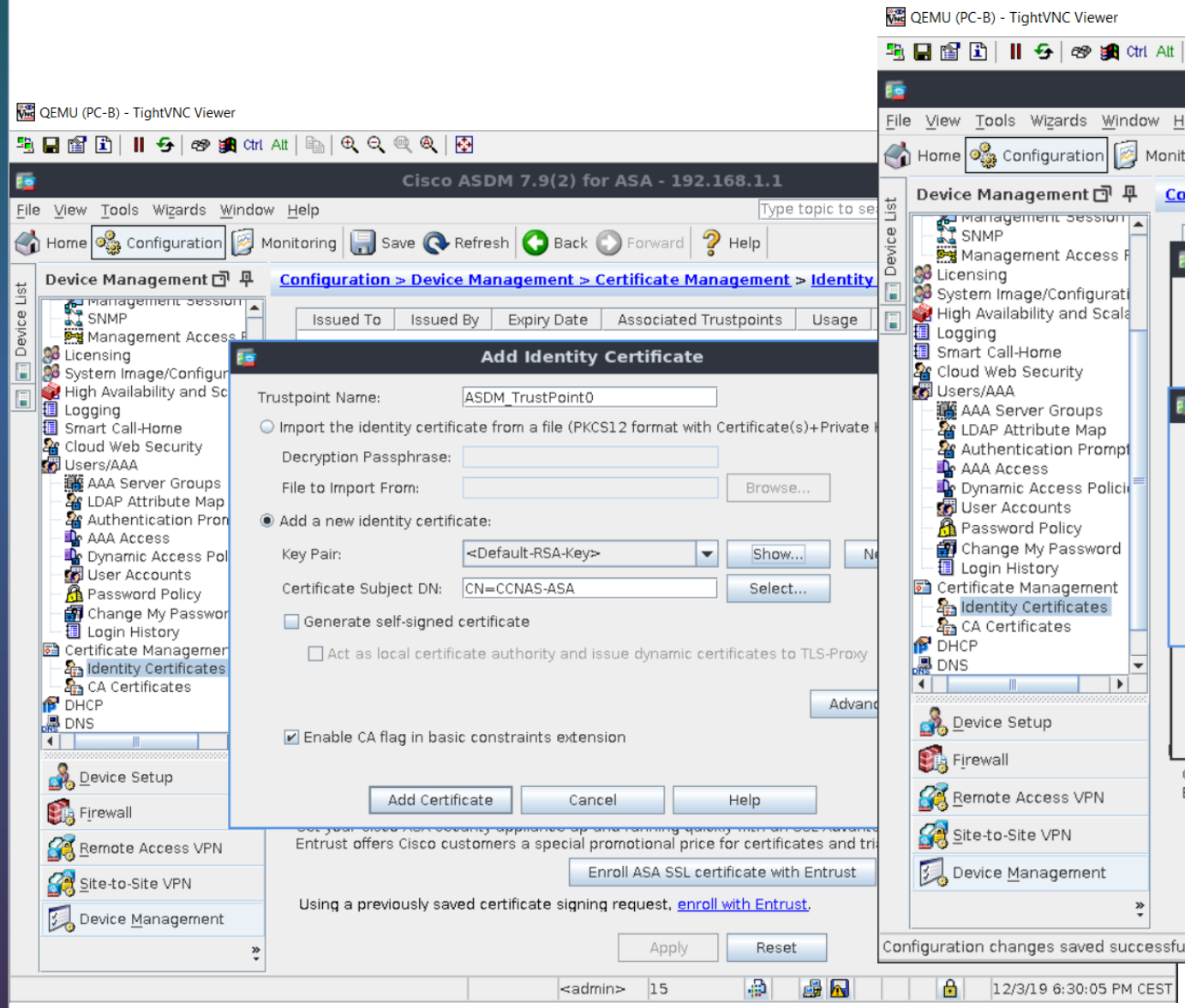
Overenie DHCP služby

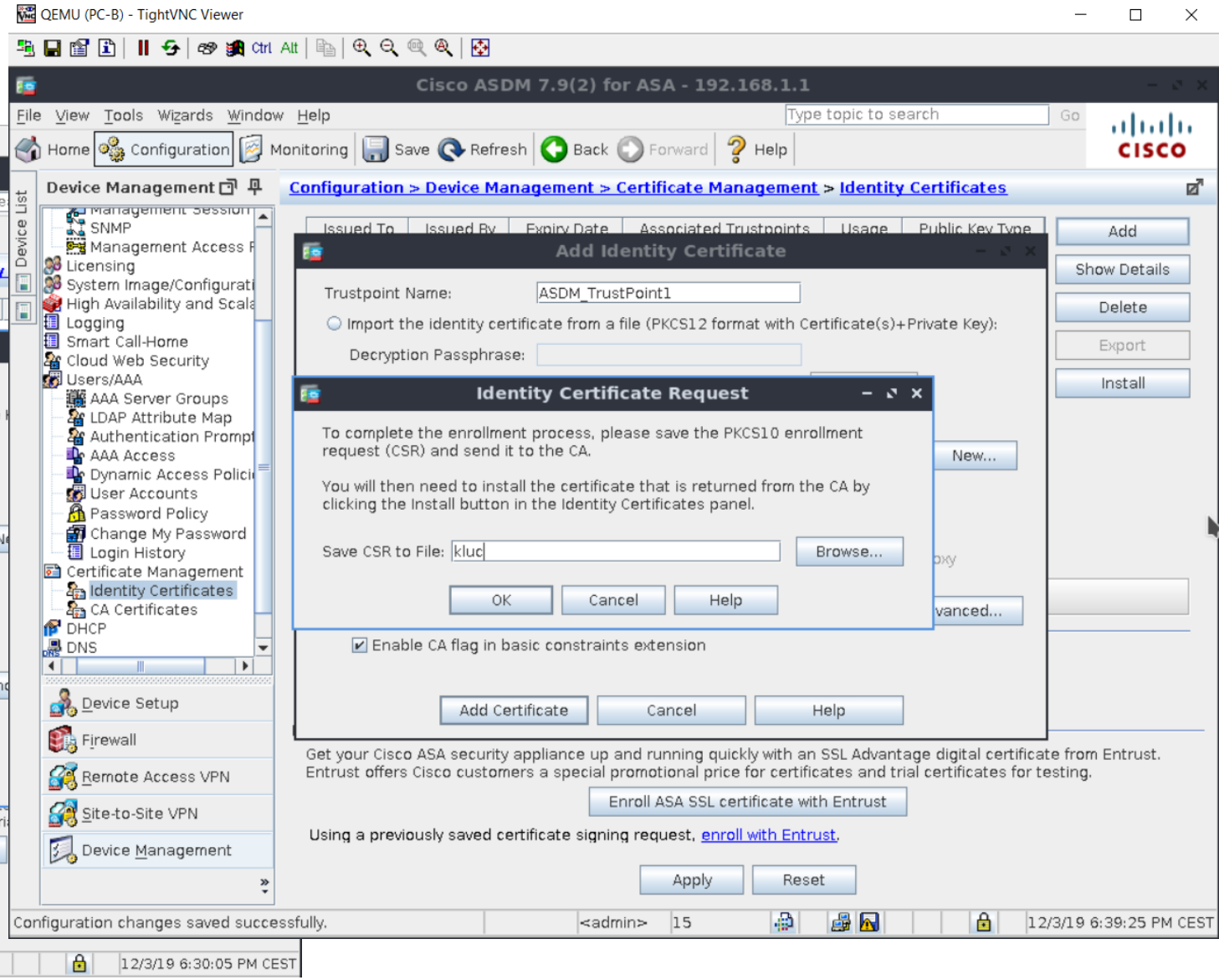


Konfigurácia AAA s využívaním lokálnej DB ASA

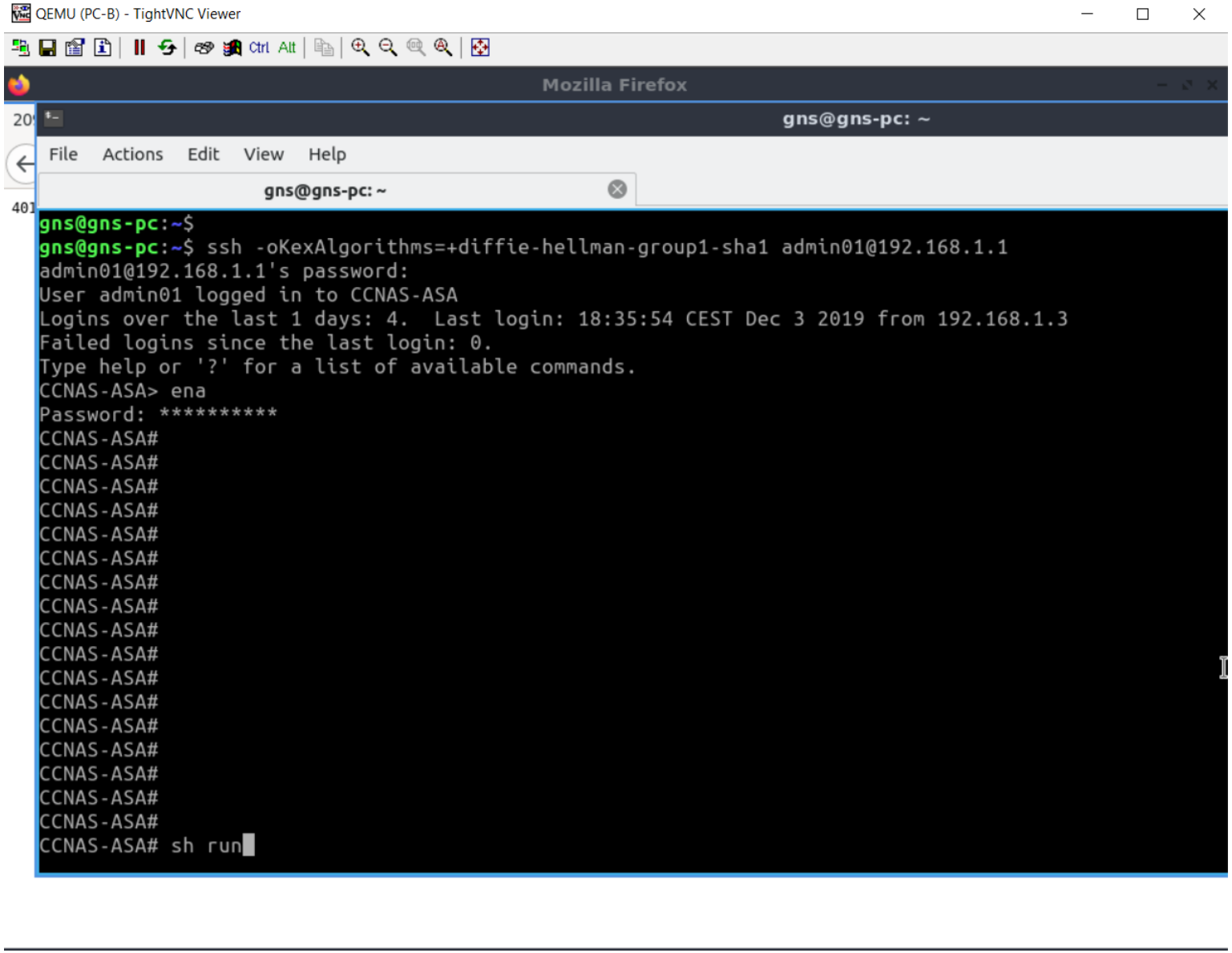


Vygenerovanie RSA kľúča

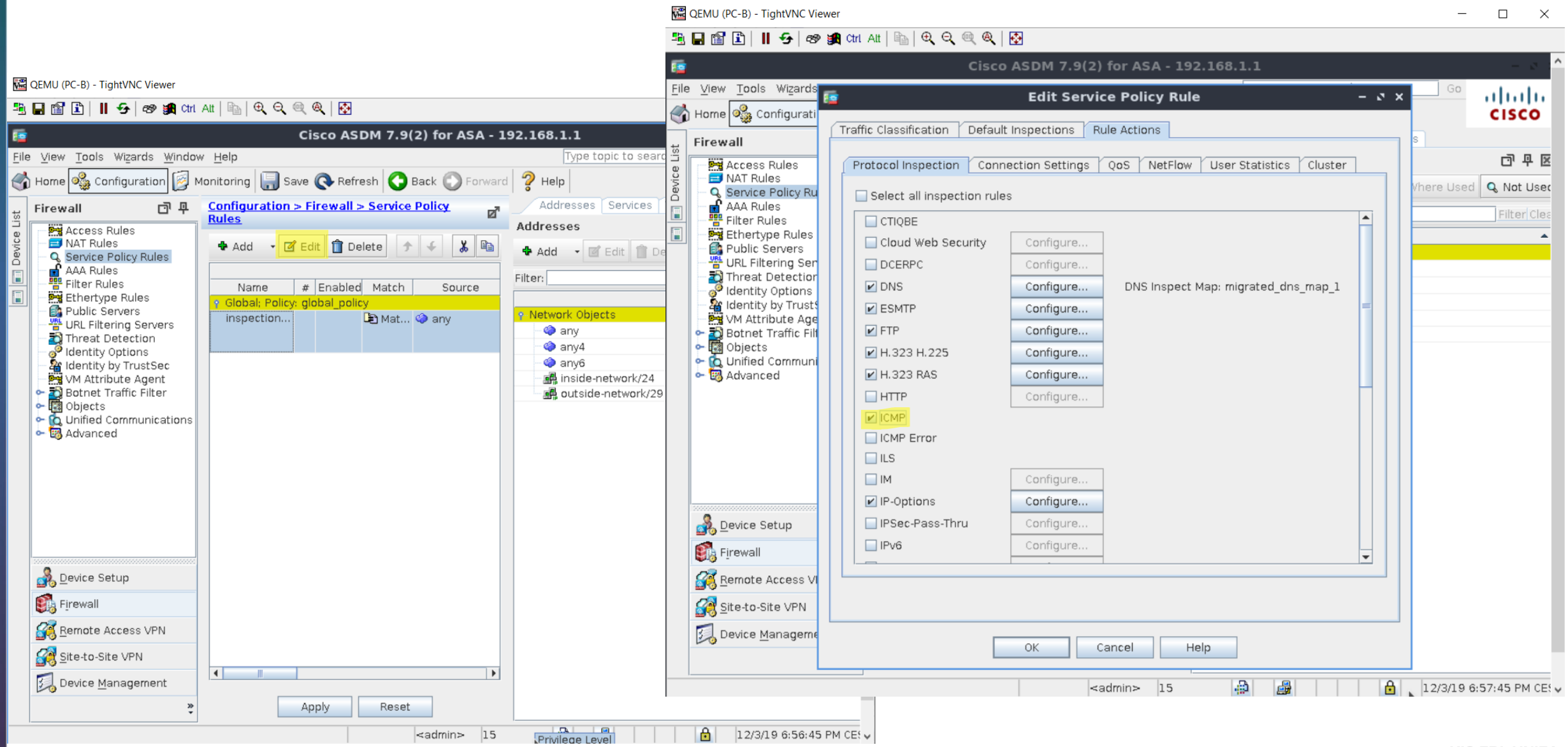




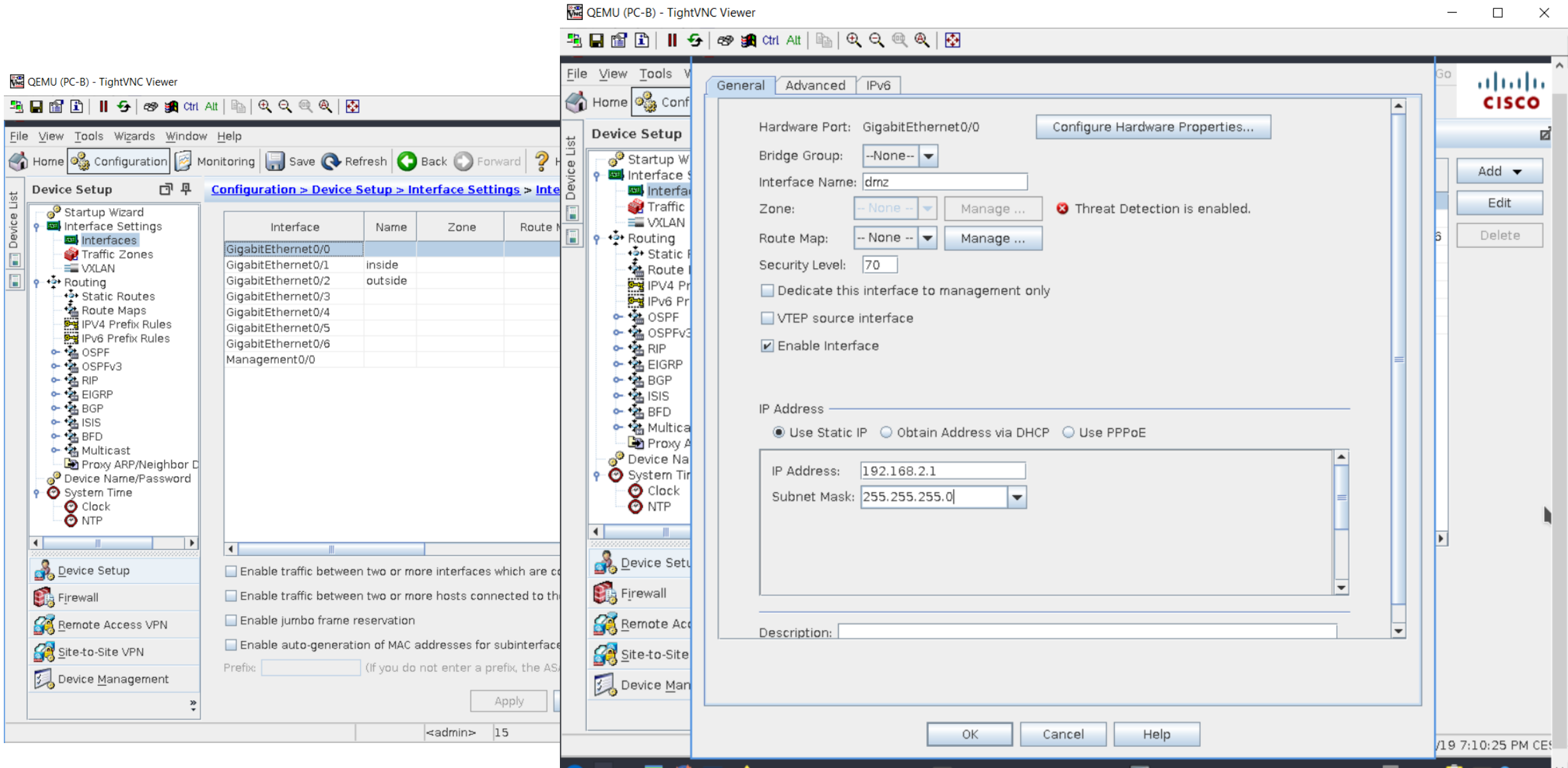
Otestovanie SSH prístupu na ASA



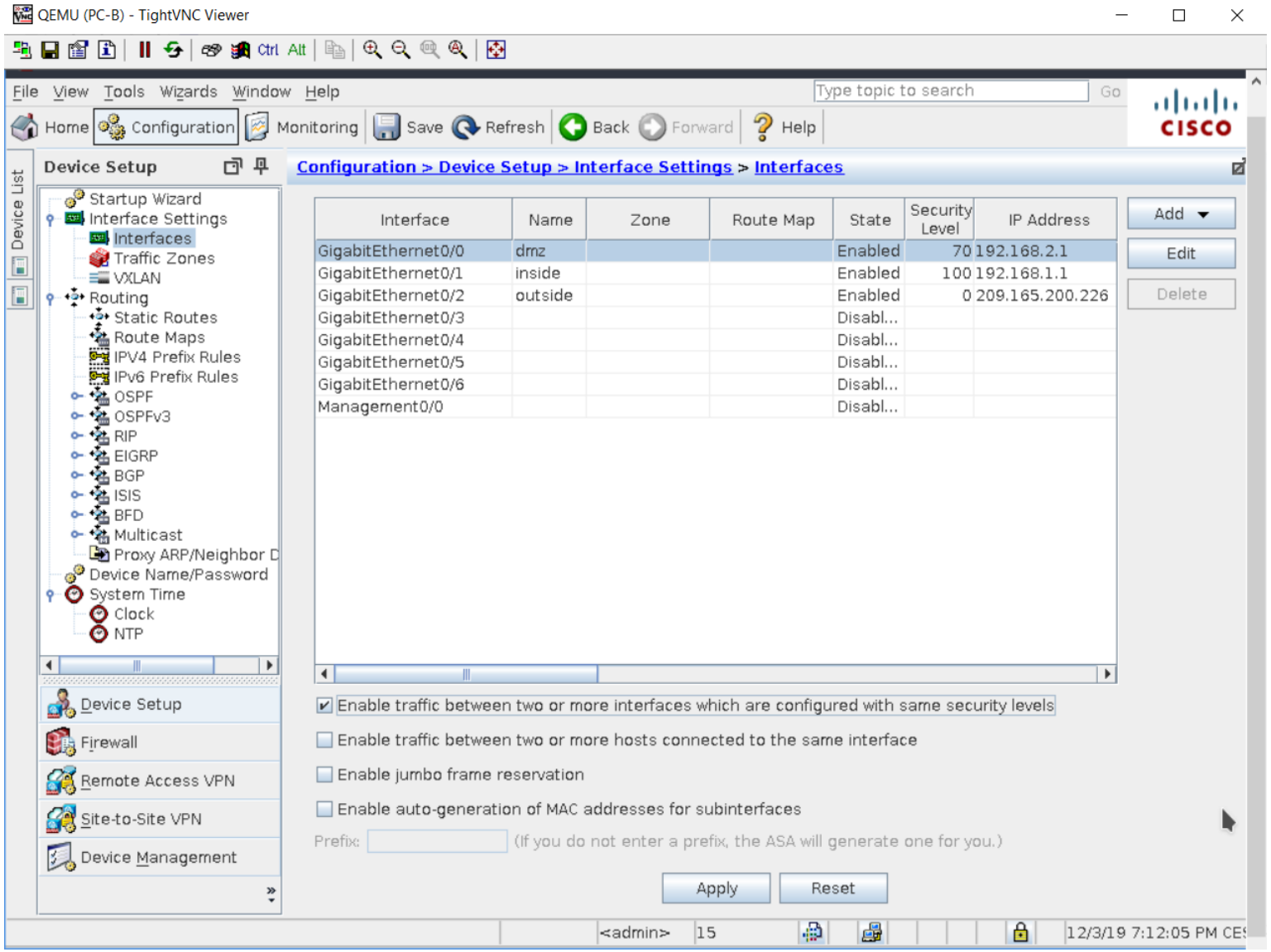
Cisco Modular Policy Framework (MPF)



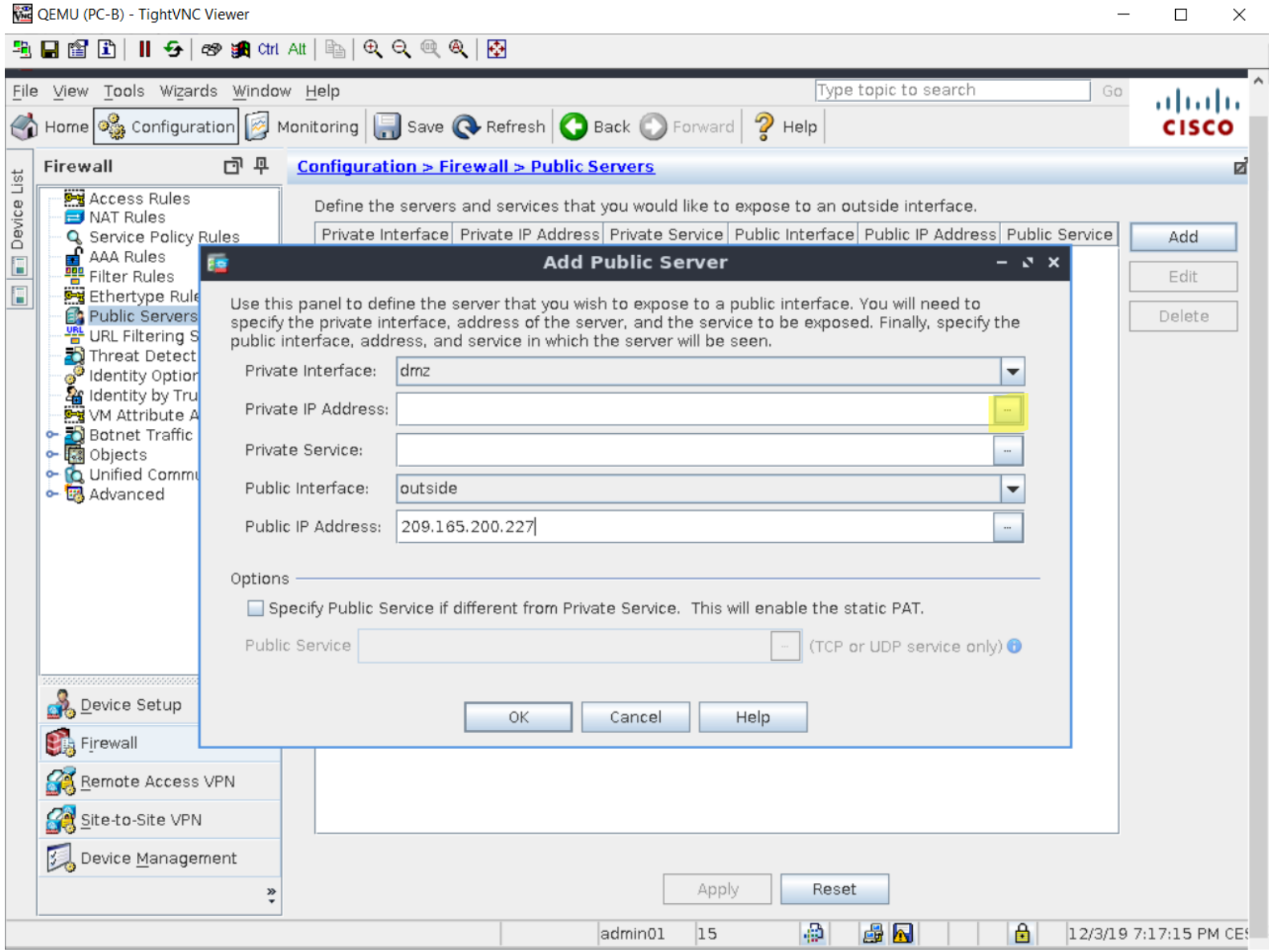
5. časť: Konfigurácia DMZ, statického NAT a ACL



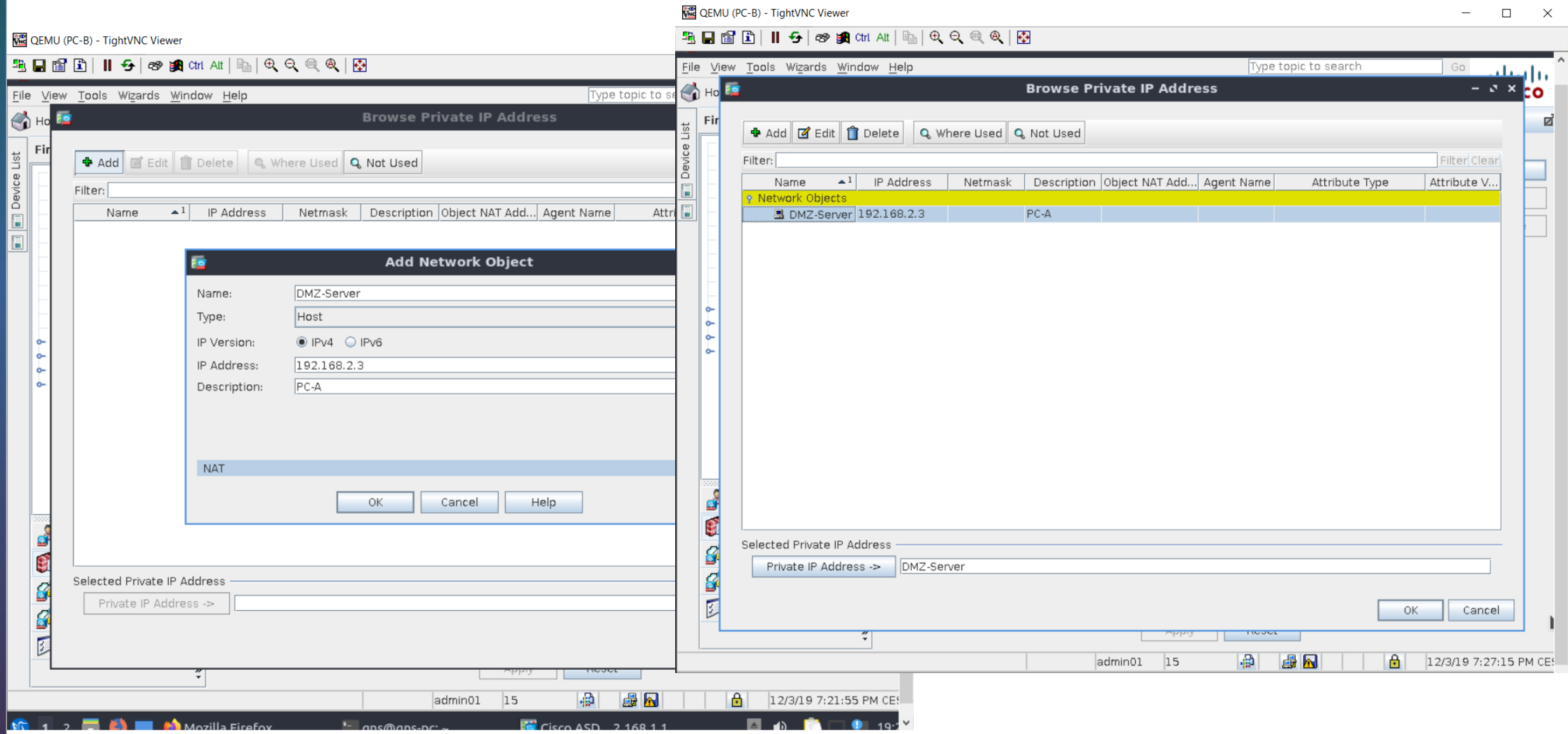
Overenie konfigurácie DMZ rozhrania



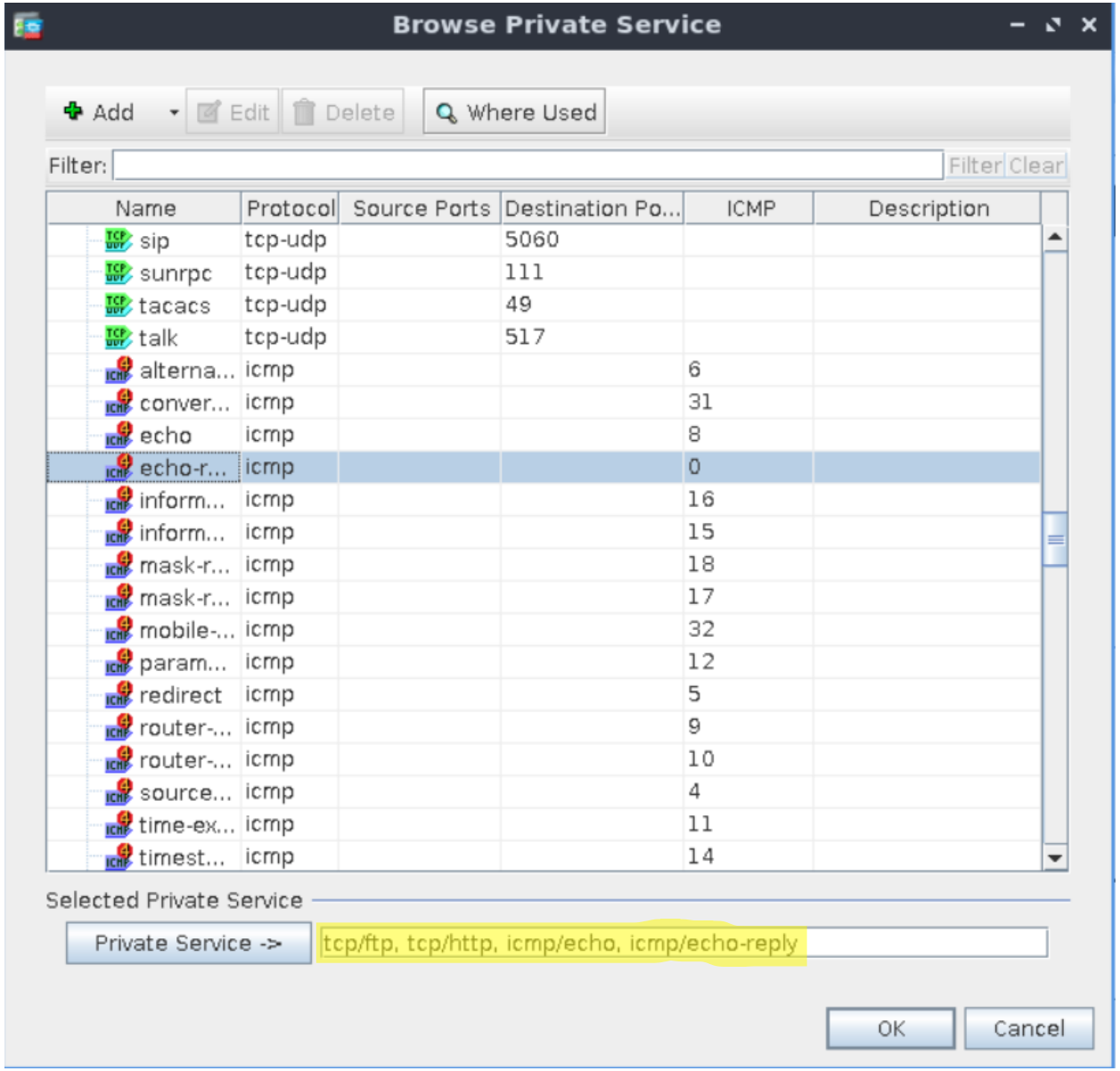
Konfigurácia DMZ servera



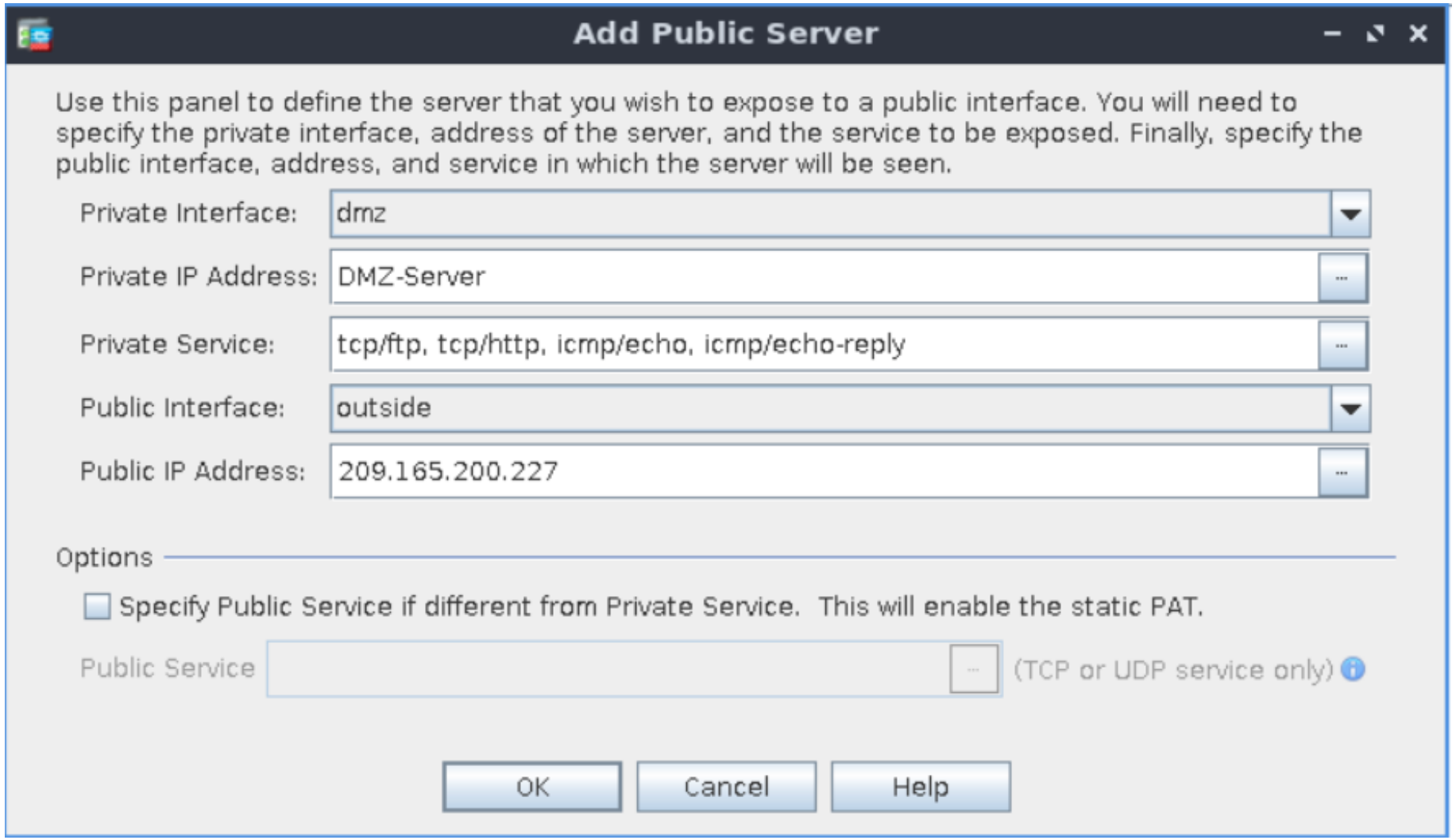
Konfigurácia DMZ servera



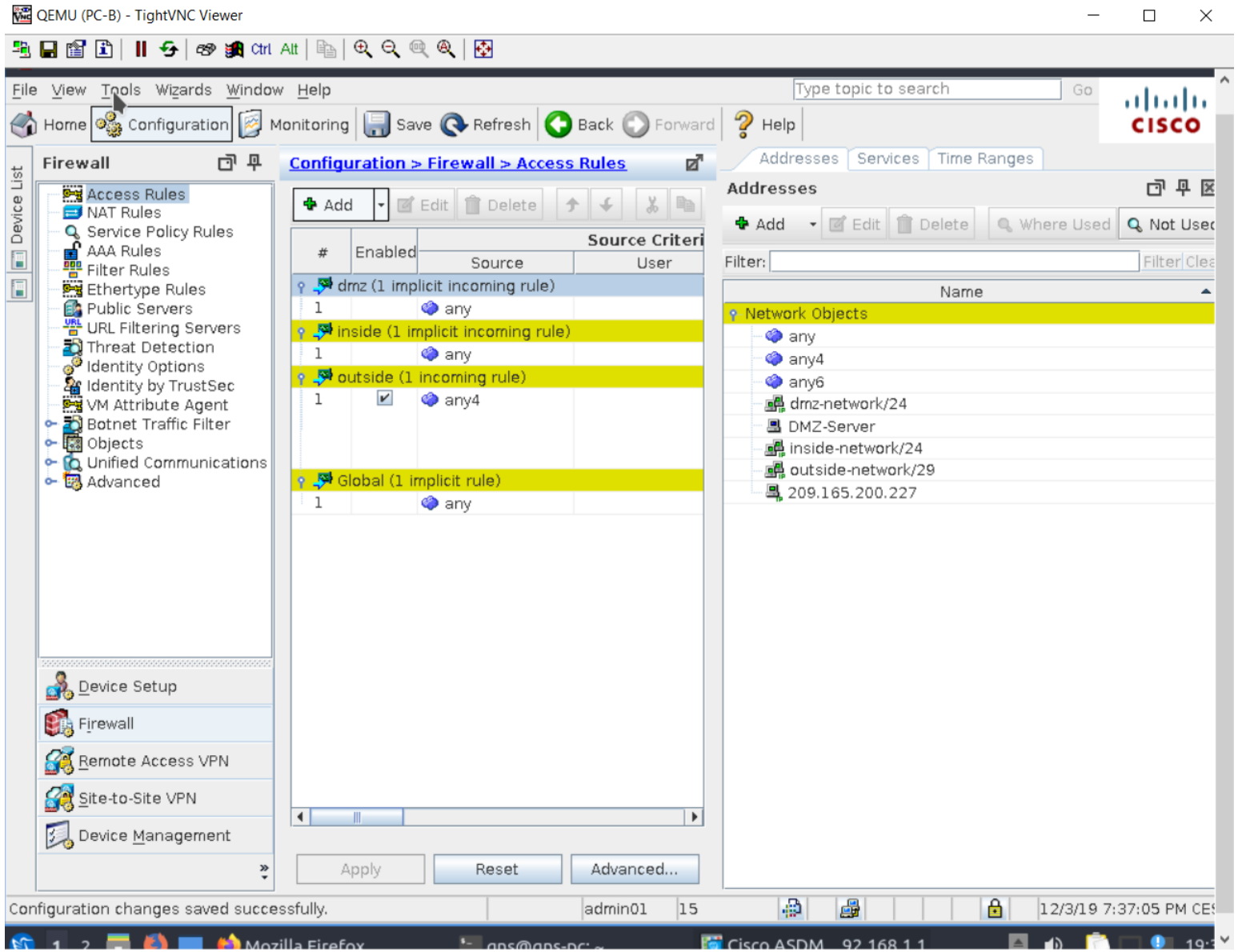
Povolenie služieb



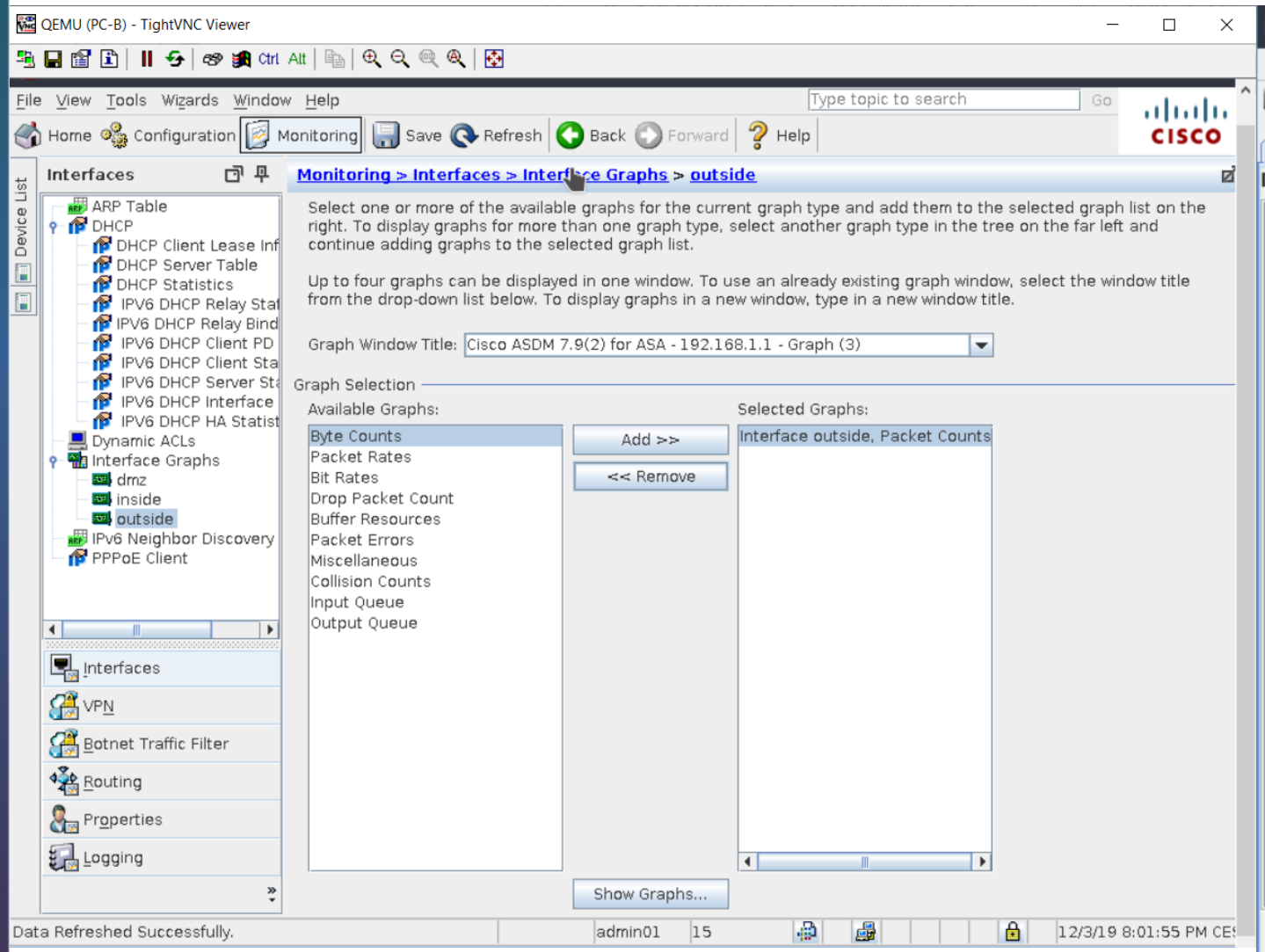
DMZ – zhrnutie

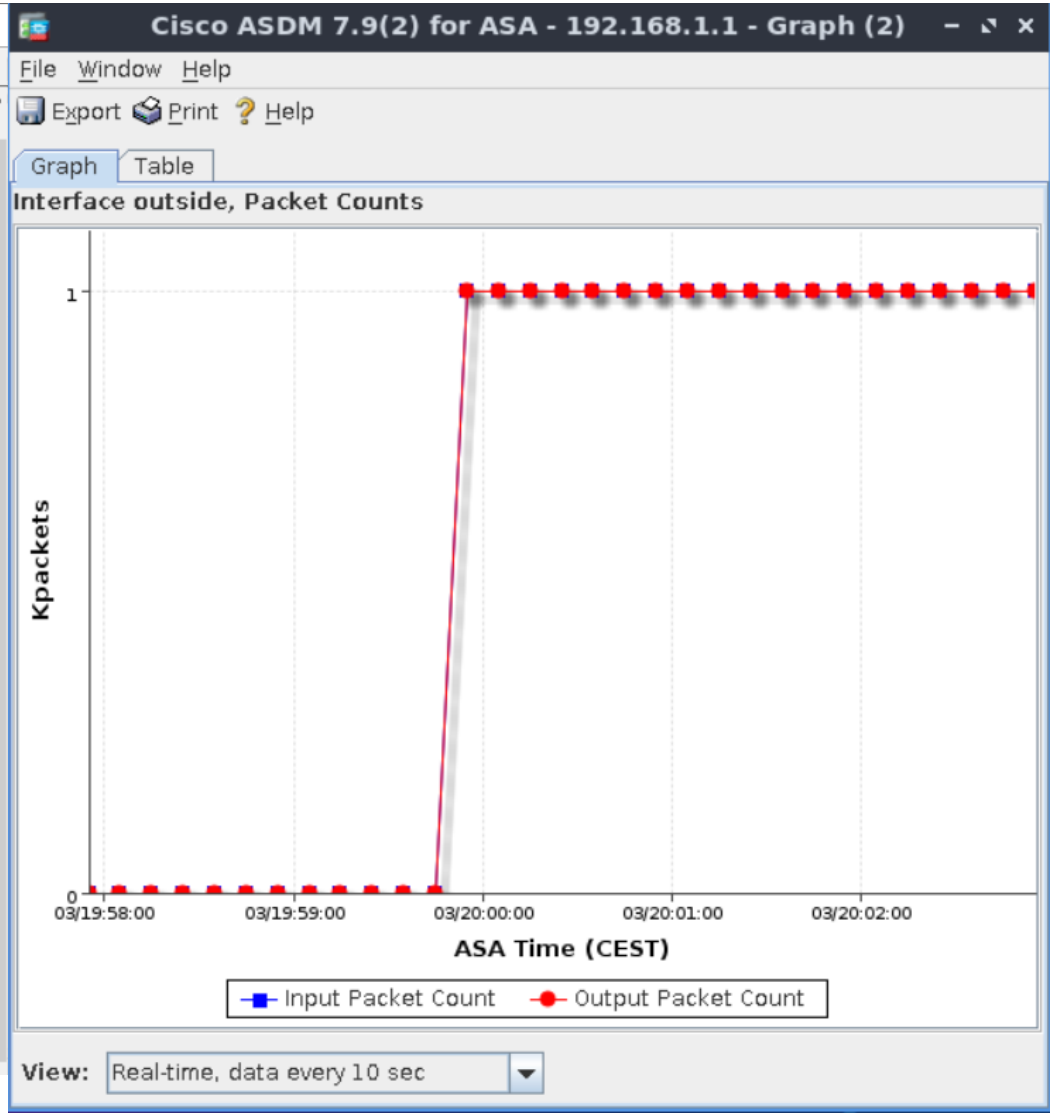


Nové ACL


QEMU (PC-B) - TightVNC Viewer
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Ethertype Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
VM Attribute Agent
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete
Enabled Source Criteri
Source User
dmz (1 implicit incoming rule)
1 any
inside (1 implicit incoming rule)
1 any
outside (1 incoming rule)
1 any4
Global (1 implicit rule)
1 any
Apply Reset Advanced...
Addresses Services Time Ranges
Addresses
Add Edit Delete Where Used Not Used
Filter:
Name
Network Objects
any
any4
any6
dmz-network/24
DMZ-Server
inside-network/24
outside-network/29
209.165.200.227
Configuration changes saved successfully.
admin01
15
12/3/19 7:37:05 PM CE
Mozilla Firefox
Cisco ASDM 7.2.1.1

Monitoring prevádzky v ASDM





10.2 ASA VPN konfigurácia

Po dokončení tejto podkapitoly by ste mali vedieť:

- Nakonfigurovať Site-to-site VPN na ASA
- Vysvetliť rozdiel medzi client-based a clientless VPN
- Nakonfigurovať remote-access VPN na ASA
- Nakonfigurovať remote-access VPN s použitím clientless SSL VPN

ASA VPN

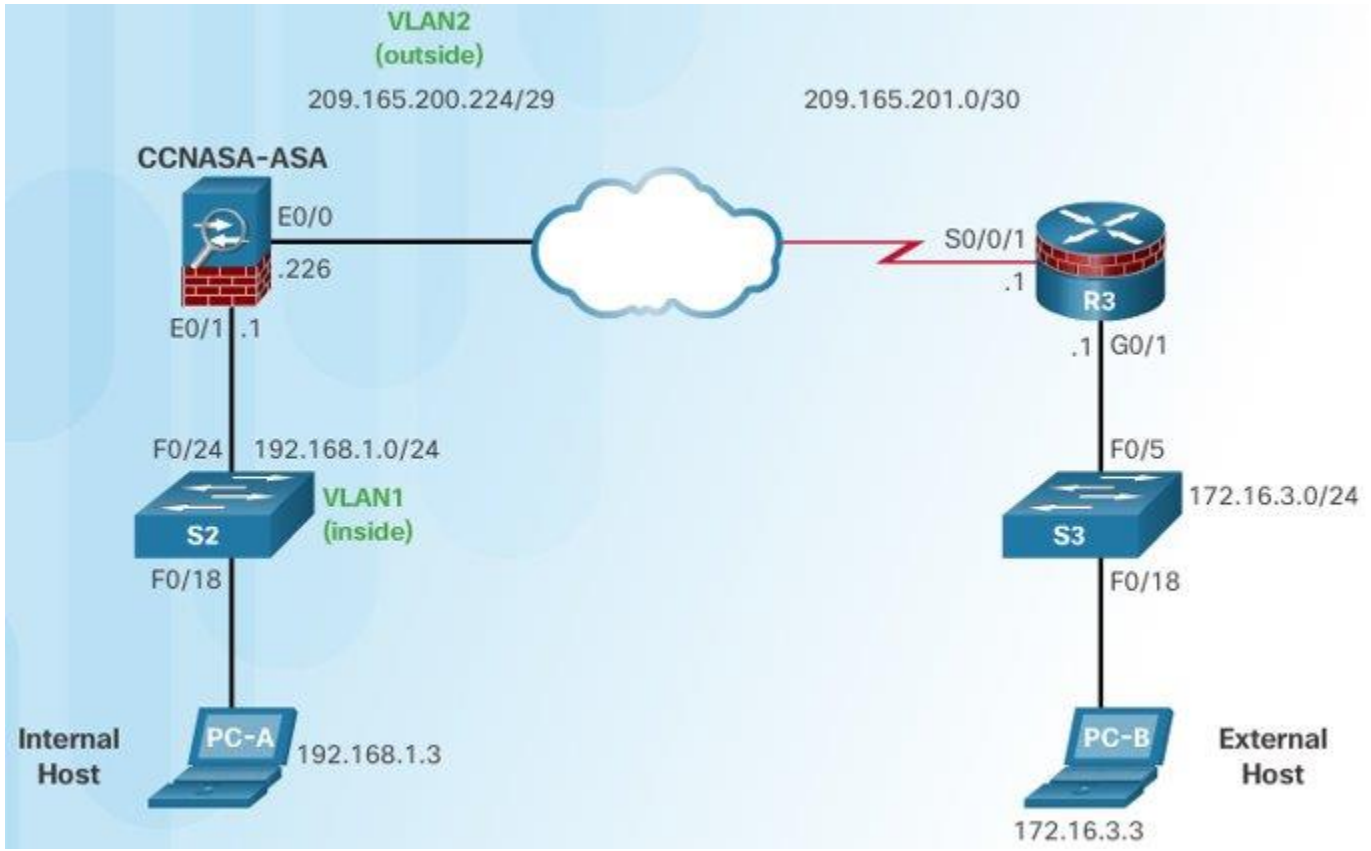
- Vytvorenie VPN spojenia medzi inou ASA alebo ISR (Integrated Service Routers)
- Komunikácia prostredníctvom vytvorením zabezpečeného pripojenia cez sieť TCP / IP (internet)
- Šifrovanie

5 krokov konfigurácie ISR

- Konfigurácia Internet Security Association and Key Management Protocol (ISAKMP) pre IKE
- Konfigurácia IPsec politiky pre IKE
- Konfigurácia ACL pre našu prevádzku
- Konfigurácia crypto map pre IPsec
- Aplikácia krypto map na interface z ktorého vychádza prevádzka

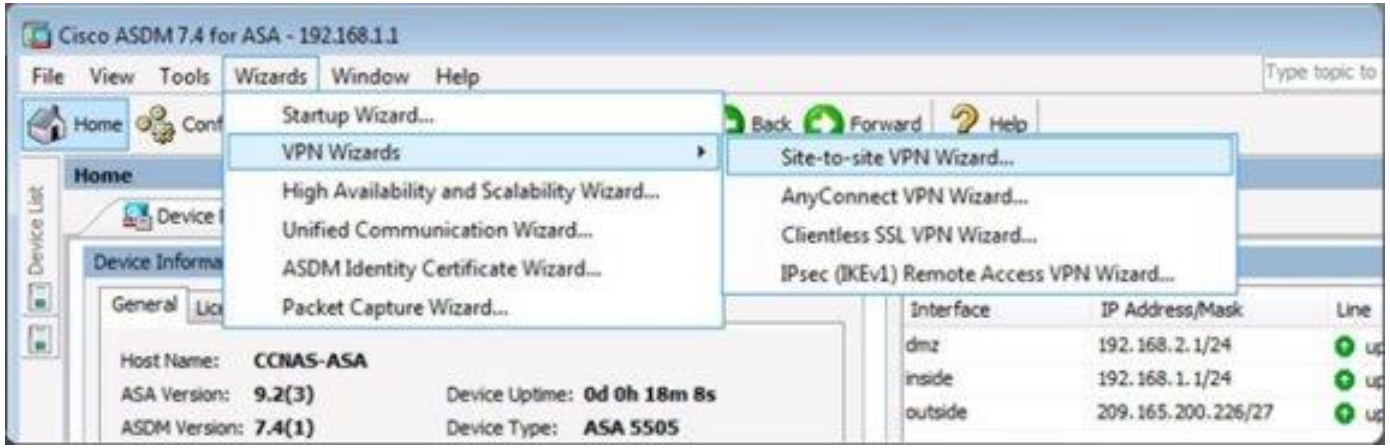
Site-to-Site VPN

- Vytvorenie šifrovaného spojenia medzi dvoma sieťami

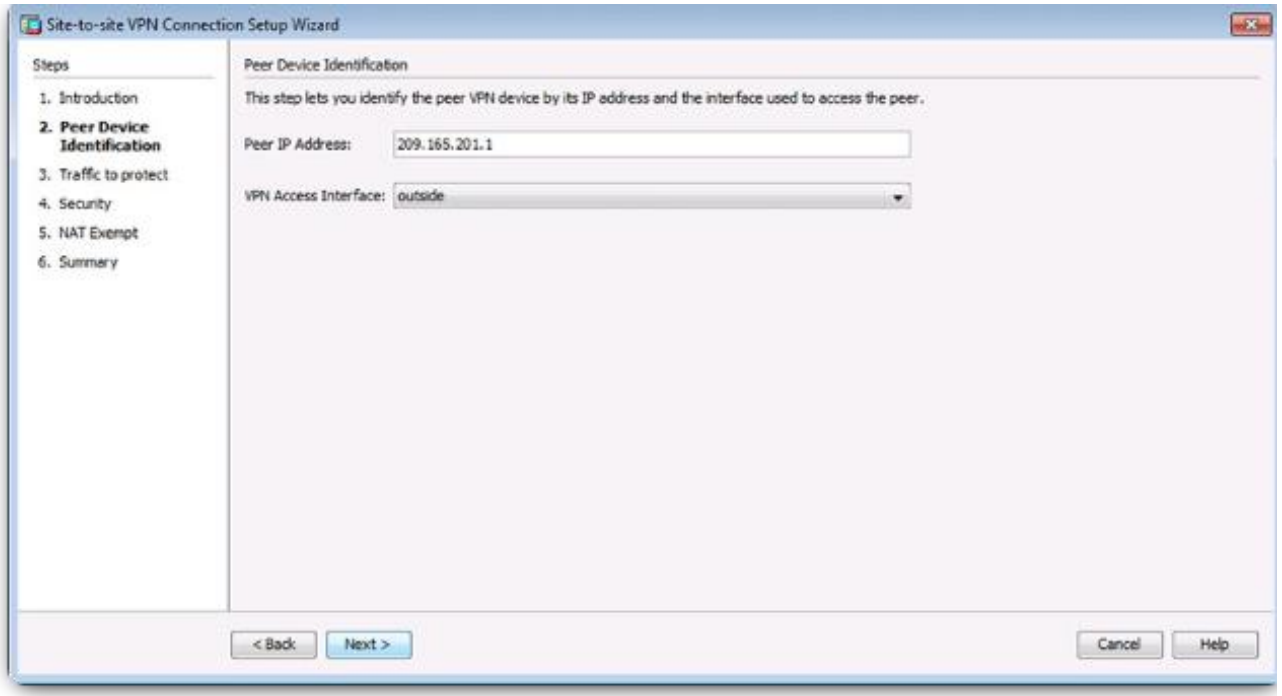


Konfigurácia ASA Site-to-site VPN použitím ASDM

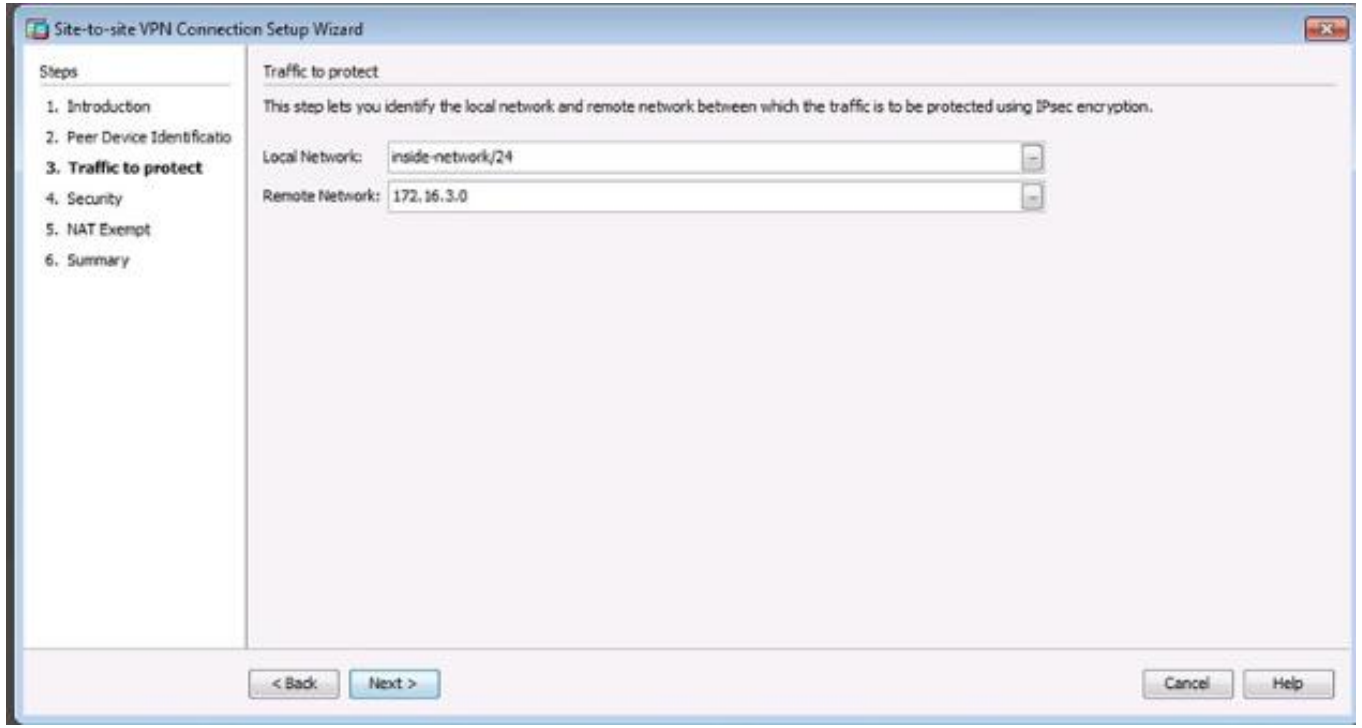
- **Step 1.** Launch the Site-to-Site VPN wizard.



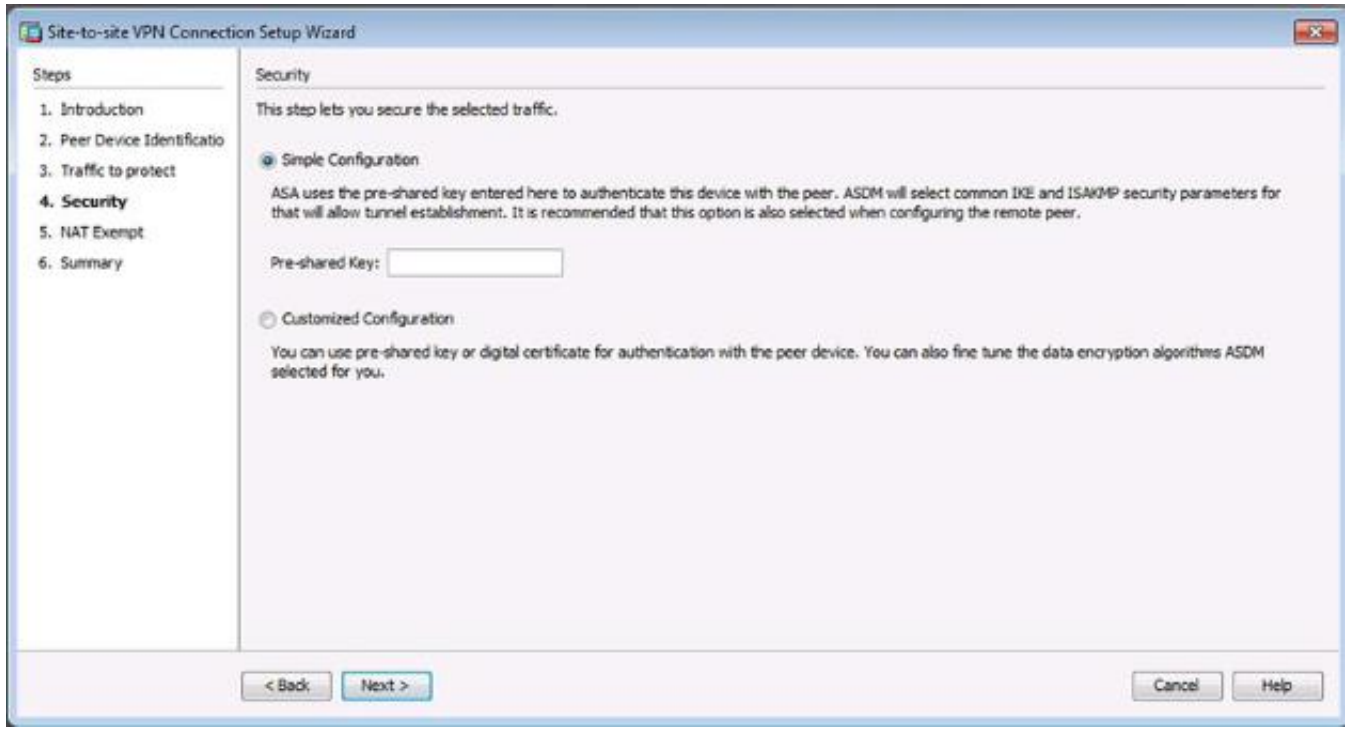
- **Step 2.** Identify the peer device



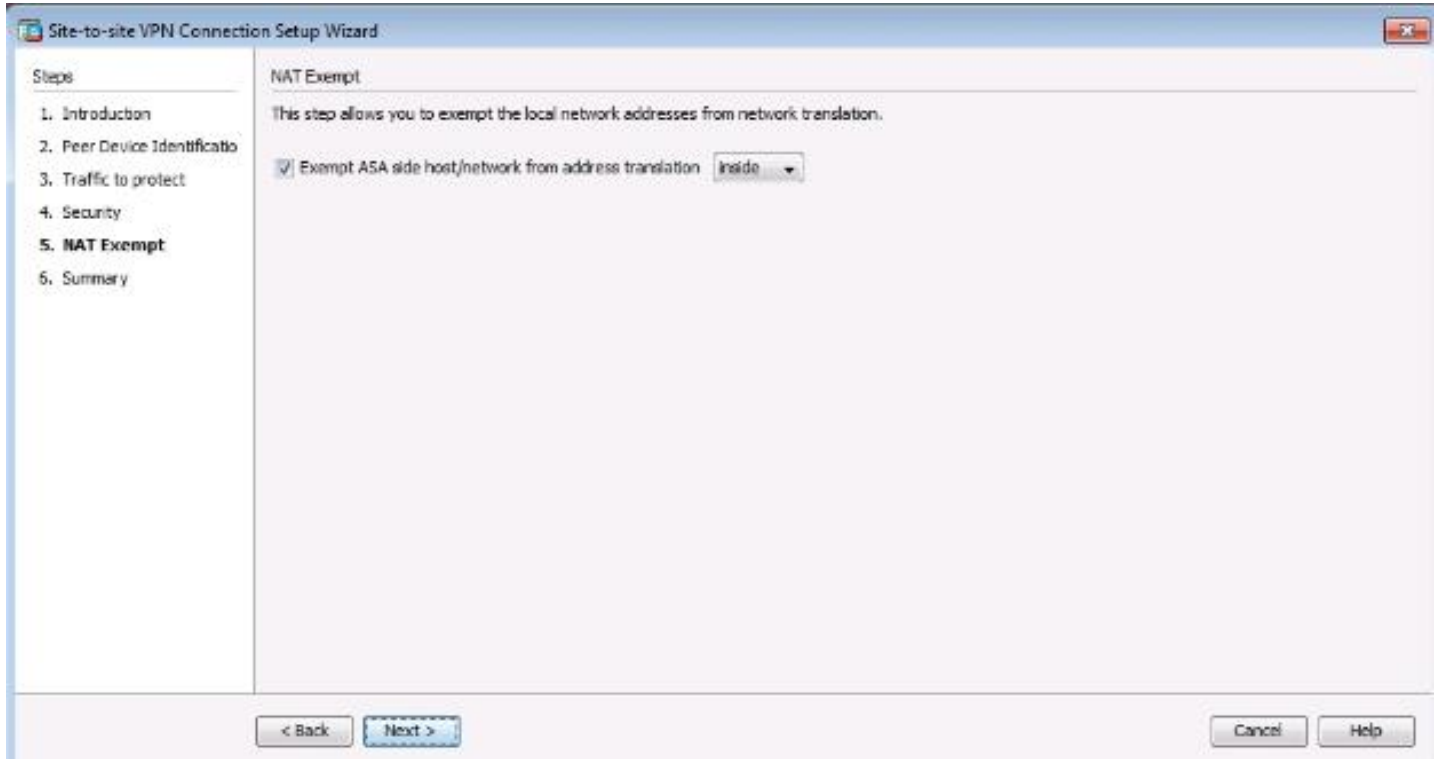
- **Step 3.** Identify interesting traffic



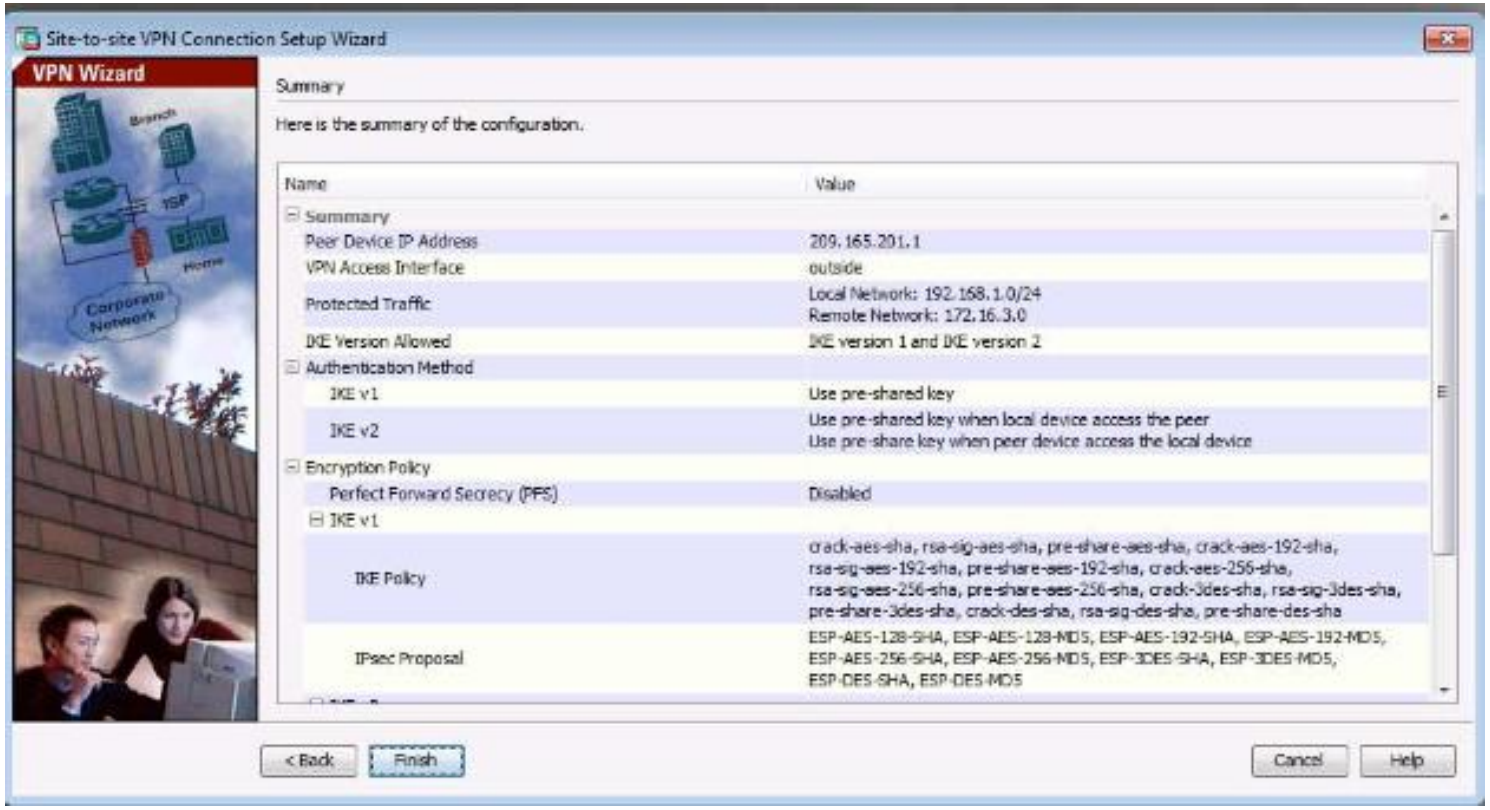
- **Step 4.** Secure the selected traffic
  - Simple Configuration
  - Customized Configuration



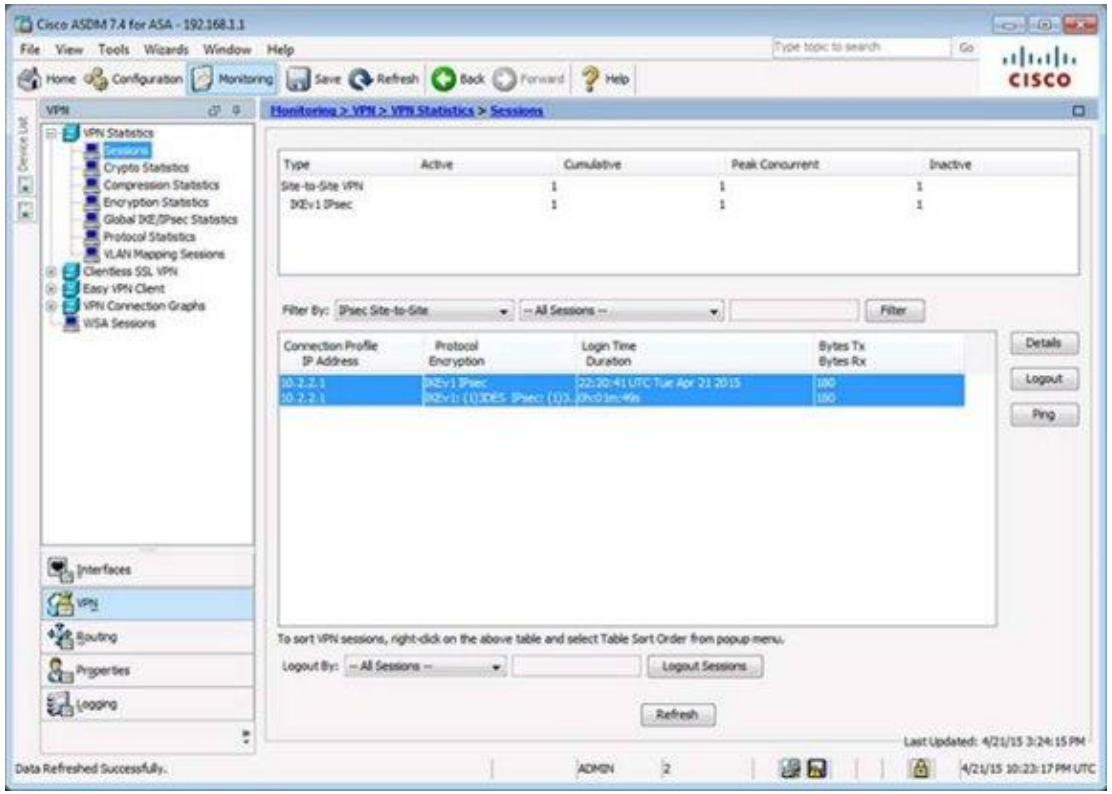
- **Step 5.** Determine whether NAT should be exempted



- **Step 6.** Verify and commit the configuration.



- **Step 7.** Verifying Site-to-Site VPNs Using ASDM

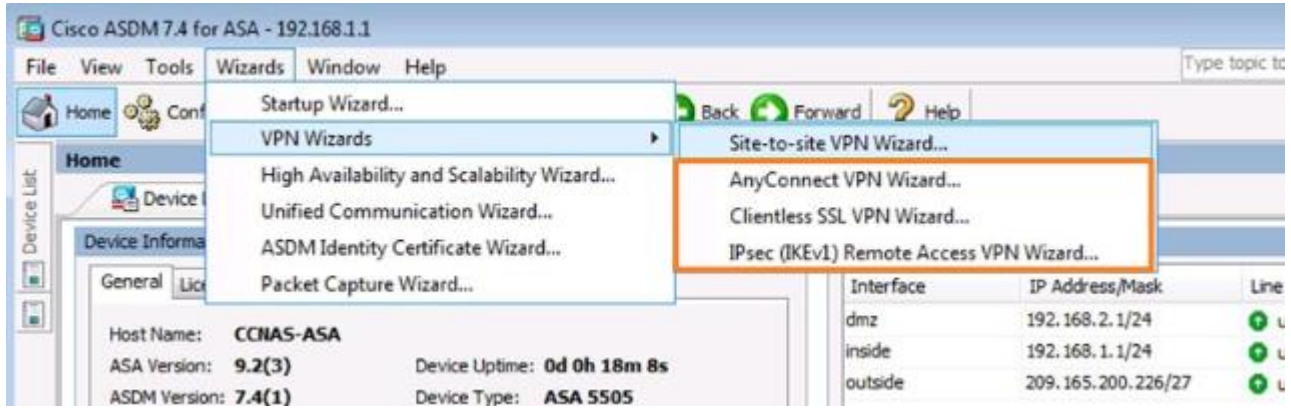


IPsec vs SSL

- Internet protocol security (Ipsec) a Secure Socket Layer (SSL) sú dve hlavné technológie využívané pre remote-access VPN
- IPsec:
  - L3 VPN technológia
  - Vyžaduje predinštalovaného VPN klienta (napr. Cisco AnyConnect)
  - Podporuje všetky typy aplikácií
  - Poskytuje silnú enkrypciu a celkovú bezpečnosť
- SSL:
  - L7 VPN technológia
  - Nevyžaduje žiadny VPN softvér
  - Umožňuje prístup k službám, súborom a webstránkam
  - Umožňuje posielanie e-mailov, používanie TCP-based aplikácií a prehliadač

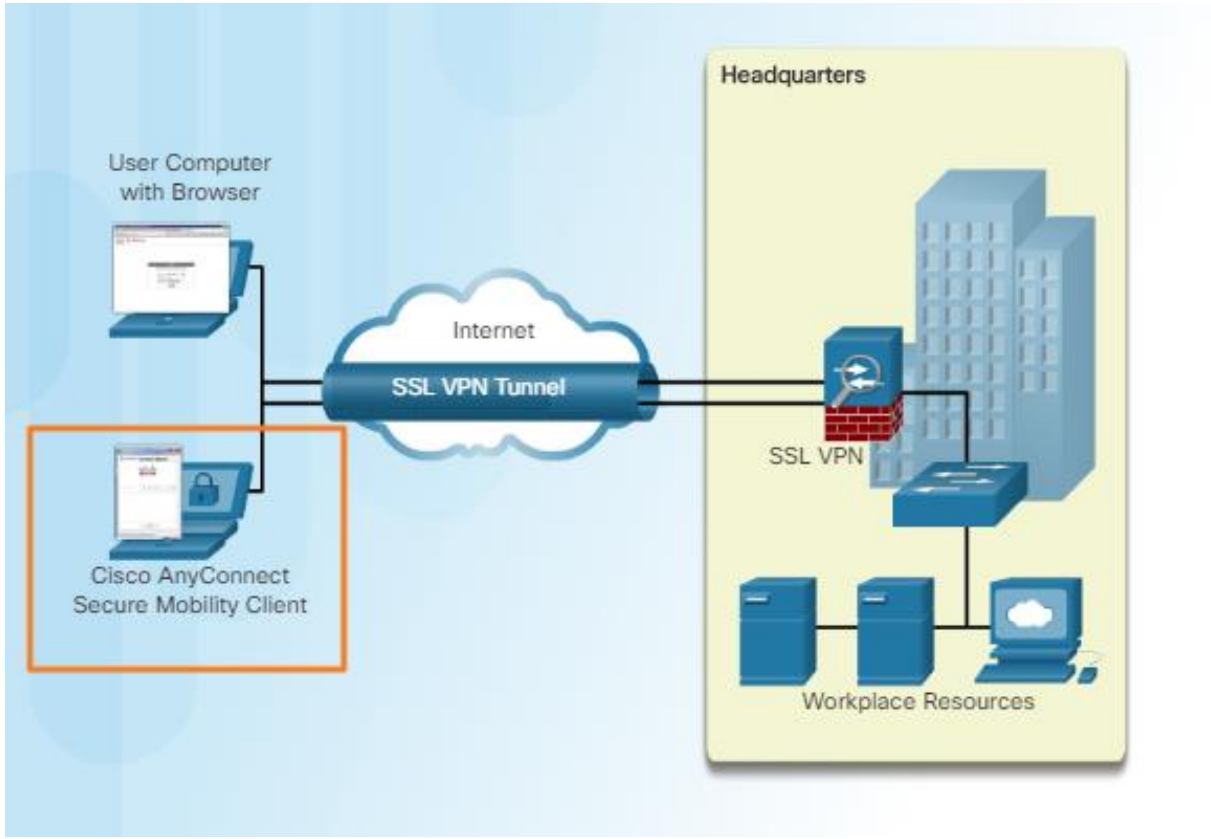
ASA SSL VPNs

- Cisco ISR a ASA poskytujú technológie IPsec a SSL VPN integrované na jedinej platforme s jednotnou správou
- ASA poskytuje tri typy riešení VPN so vzdialeným prístupom
- IKEv1 je implementovaný pri pripájaní k starším klientom VPN, ako je napríklad klient Cisco VPN
- IKEv2 je implementovaný pre novších klientov VPN, ako je napríklad klient Cisco AnyConnect Secure Mobility Client



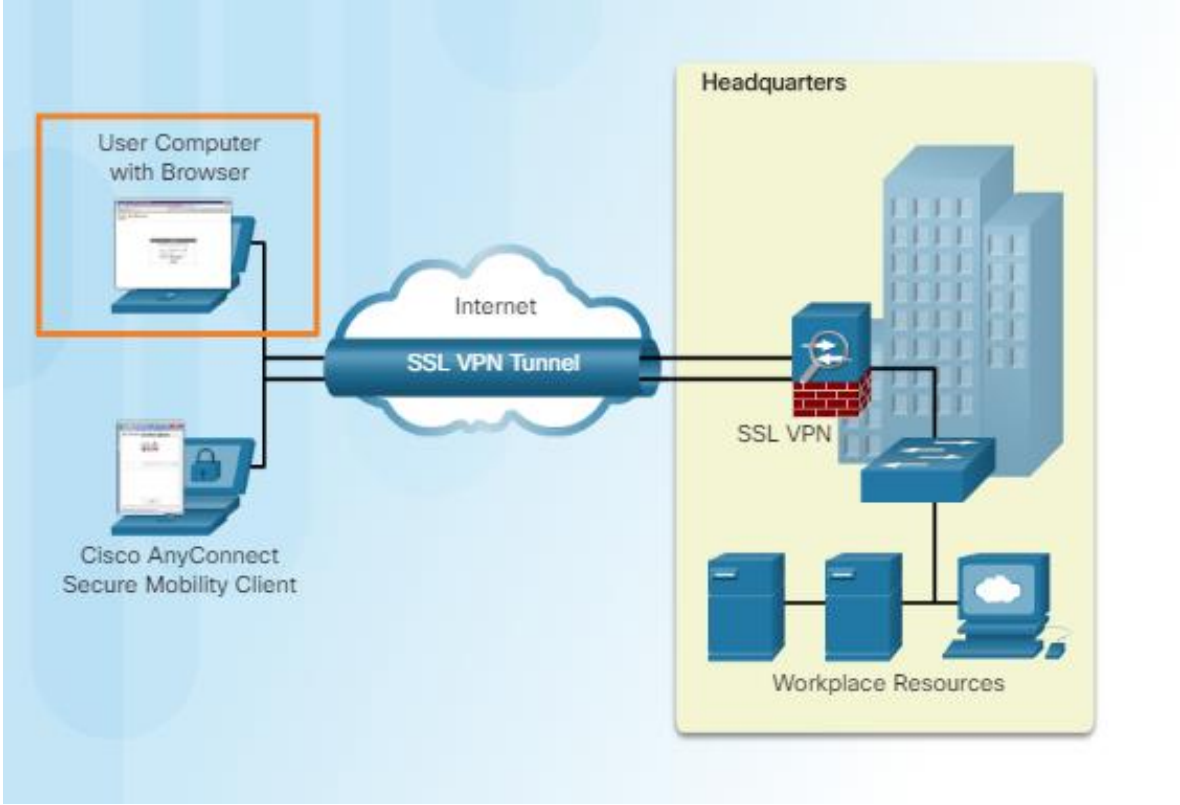
Client-Based SSL VPN

- Client-Based SSL VPN poskytuje úplné tunelové riešenie
- Vyžaduje sa inštalácia klientskej aplikácie na koncové zariadenie
- Poskytuje úplný prístup ku zdrojom vo firemnej sieti
- Cisco poskytuje Cisco AnyConnect Secure Mobility Client



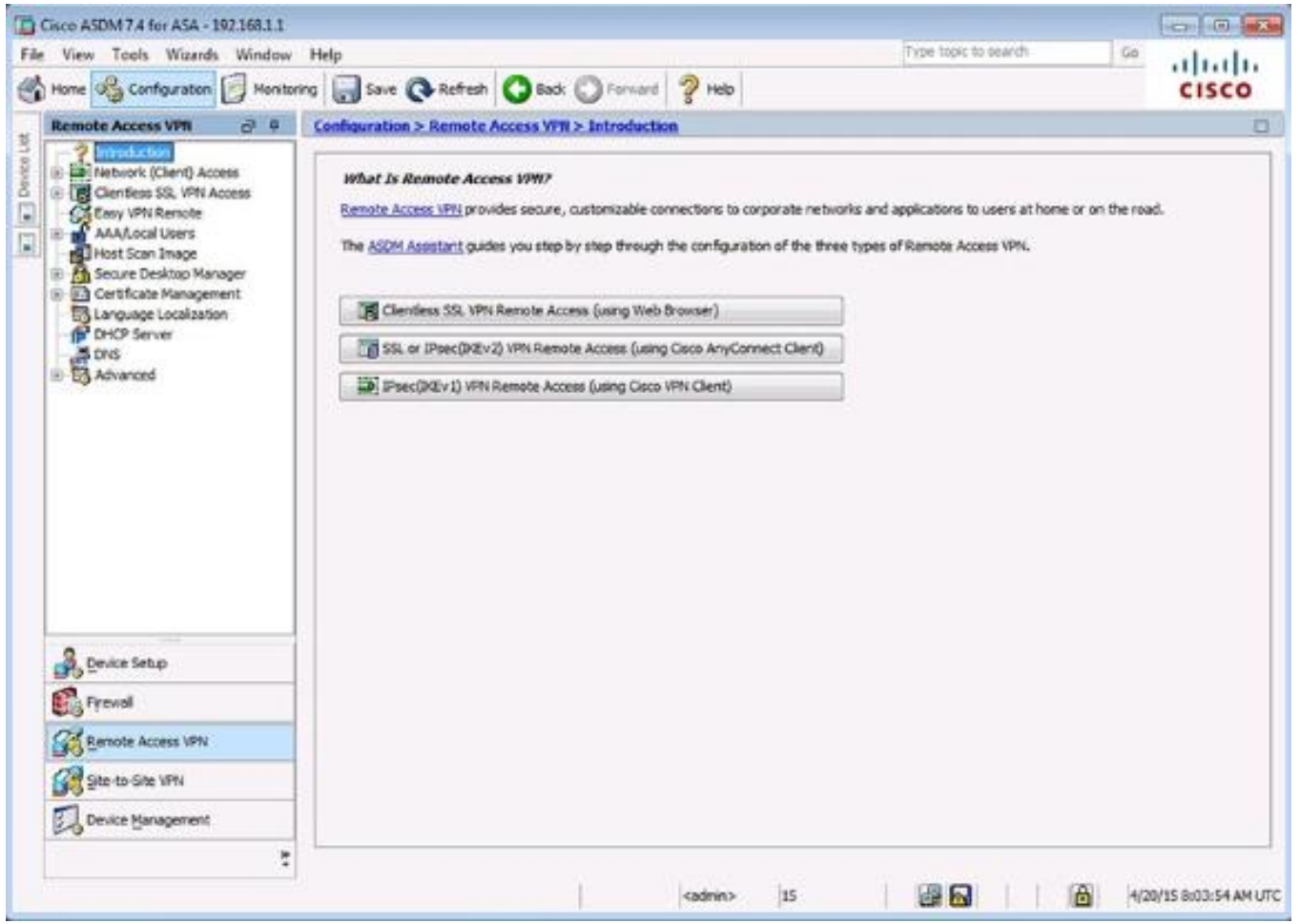
Clientless SSL VPN

- Clientless model umožňuje prístup k zdrojom vo firemnej sieti
- VPN so vzdialeným prístupom k ASA prostredníctvom webového prehliadača
- Cisco ASA je používaná ako proxy zariadenie ku zdrojom v sieti
- Cisco ASA poskytuje web portal interface na navigáciu v sietí s využitím port-forwardingu
- Jednoduchšie na nasadenie ako client-based SSL VPN



Konfigurácia Clientles SSL VPN na ASA

- ASDM poskytuje dva nástroje na počiatočnú konfiguráciu clientless SSL VPN na ASA:
  - ASDM Assisstant
  - VPN wizard



Lab 3 - Configure Clientless Remote Access SSL VPNs Using ASA- 5506-X ASDM

- Konfigurácia SSL VPN používateľského rozhrania
- Konfigurácia autentifikácie
- Konfigurácia group policy pre VPN
- Konfigurácia bookmark list-u (URL adresy, ktoré sú nakonfigurované na používanie vo webovom portáli clientless SSL VPN)
- Overenie

Ďakujem za pozornosť