



Kapitola 10: Pokročilé ovládanie ASA cez ASDM GUI

CCNA Security v2.0



Networking
Academy



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

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home Device Dashboard Firewall Dashboard

Device Information

General License

Host Name: **ciscoasa**

ASA Version: **9.2(3)** Device Uptime: **0d 0h 28m 10s**

ASDM Version: **7.4(1)** Device Type: **ASA 5505**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **128 MB** Total Memory: **512 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	4

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 [Details](#)

System Resources Status

CPU Usage (percent)

7%

Memory Usage (MB)

272 MB

Traffic Status

Connections Per Second Usage

'inside' Interface Traffic Usage (Kbps)

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

Enable Logging

Device configuration loaded successfully.

<admin> 15 4/3/15 7:10:36 AM UTC

Domovské menu - ASDM dashboard

Menu bar

Tool bar

Device list

Status bar

QEMU (PC-B) - TightVNC Viewer

Cisco ASDM 7.9(2) for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

Home

Device Dashboard Firewall Dashboard

Device Information

General License Virtual Resources

Host Name: **ciscoasa**
ASA Version: **9.9(2)25** Device Uptime: **0d 2h 30m 41s**
ASDM Version: **7.9(2)** Device Type: **ASAv**
Firewall Mode: **Routed** Number of vCPUs: **1**
Total Flash: **8192 MB** Total Memory: **2048 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	2
outside	no ip address	up	up	0

Select an interface to view input and output Kbps

VPN Summary

IPsec 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0 [Details](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

1623 MB

Latest ASDM Syslog Messages

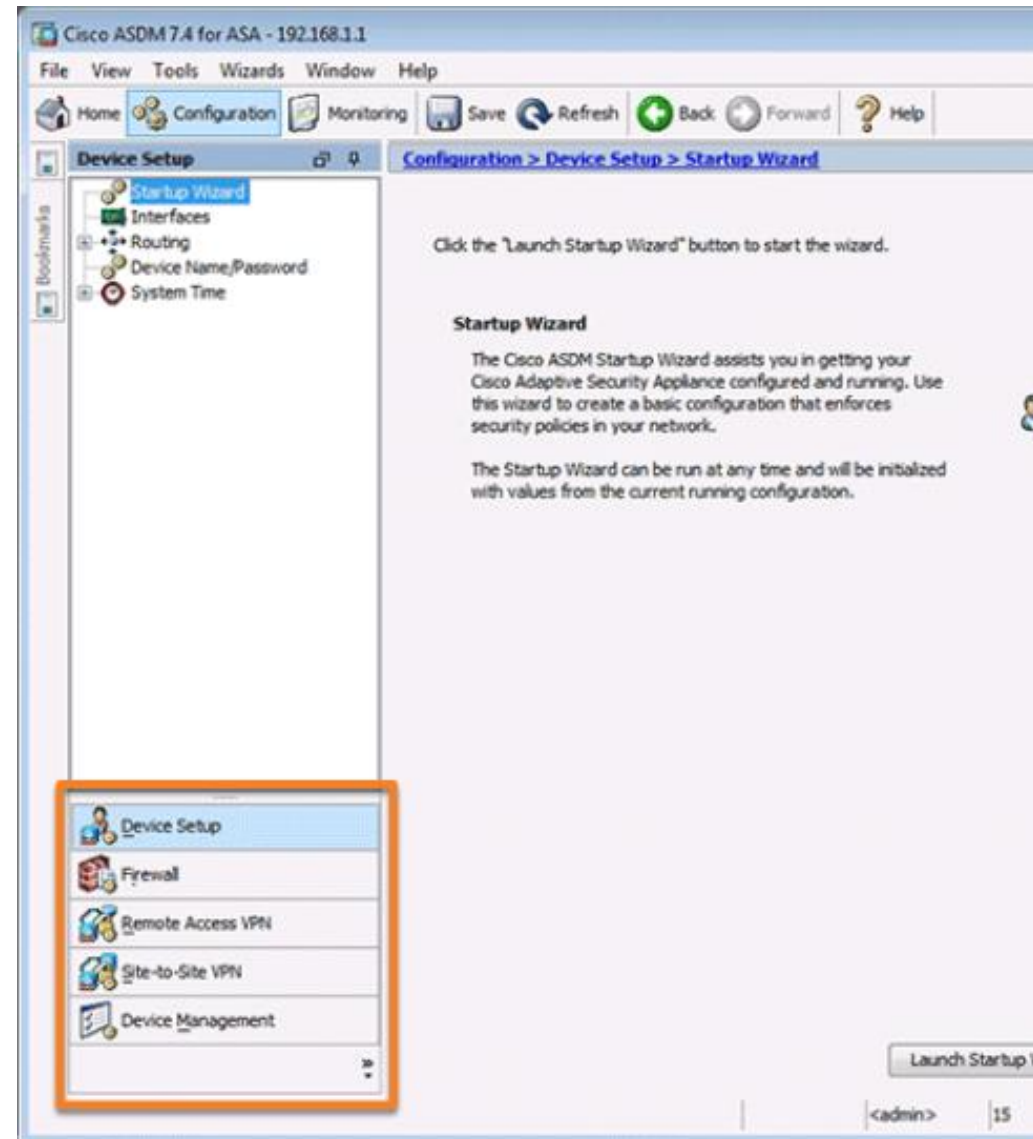
ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

[Enable Logging](#)

Device configuration loaded successfully. <admin> 15 12/2/19 8:38:04 PM UTC

Domovské menu - ASDM dashboard

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



ASDM – monitoring view

The screenshot shows the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The 'Monitoring' tab is selected, and the 'ARP Table' is displayed. The ARP table contains one entry for the 'inside' interface with IP address 192.168.1.3 and MAC address 0050.50be.73e1. The 'Proxy Arp' column is set to 'No'. The 'Refresh' button is visible at the bottom of the table area. The 'Clear Dynamic ARP Entries' button is also present. The status bar at the bottom shows the user is logged in as 'admin' and the system was last updated on 4/11/15 at 7:35:17 AM.

Interface	IP Address	MAC Address	Proxy Arp
inside	192.168.1.3	0050.50be.73e1	No

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:
 - Vnútročné 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)

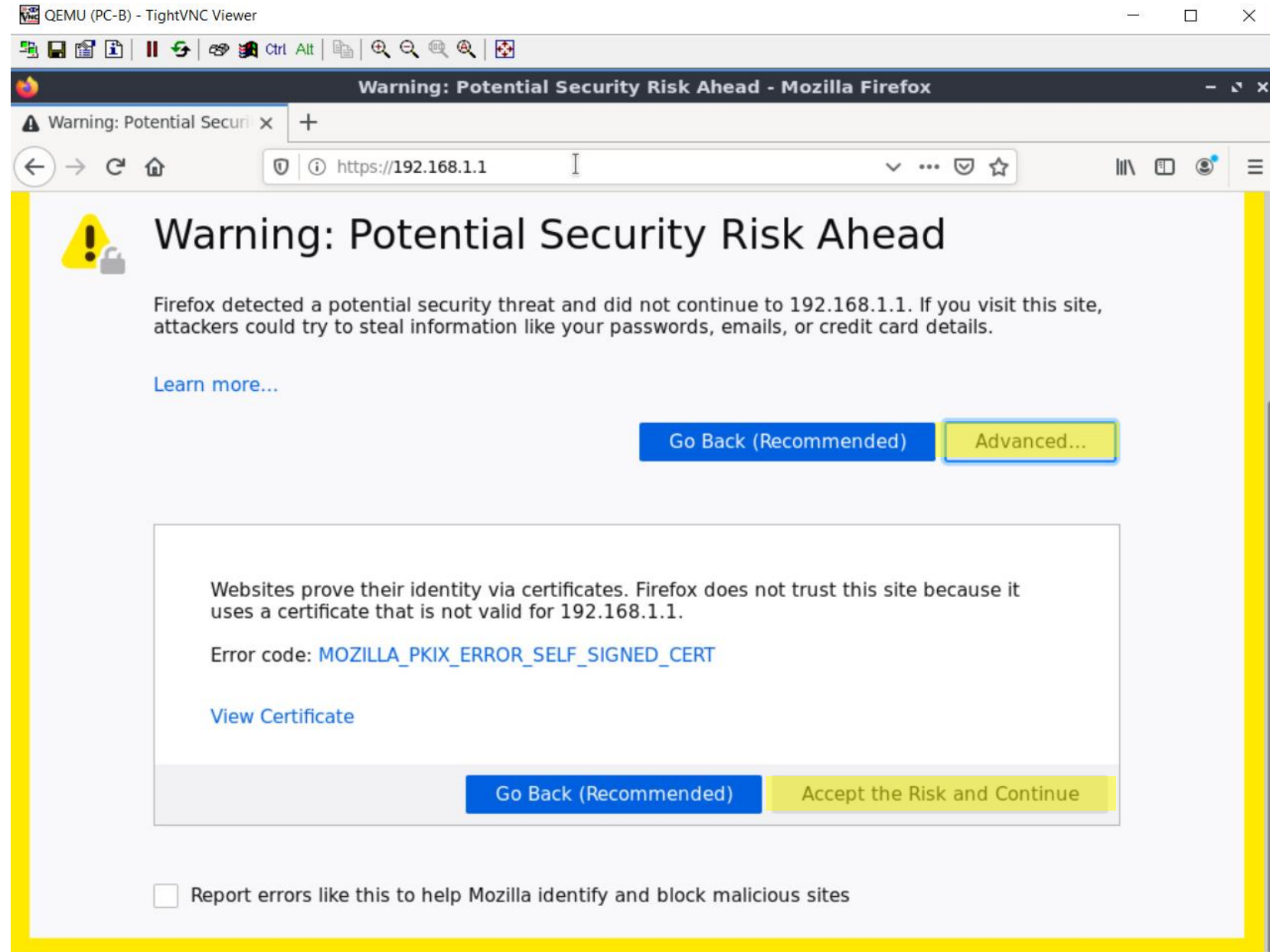
```
ciscoasa# conf t
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# 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 ASA v

- Na ASA nakonfigurujte:
 - Vnútorne 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?

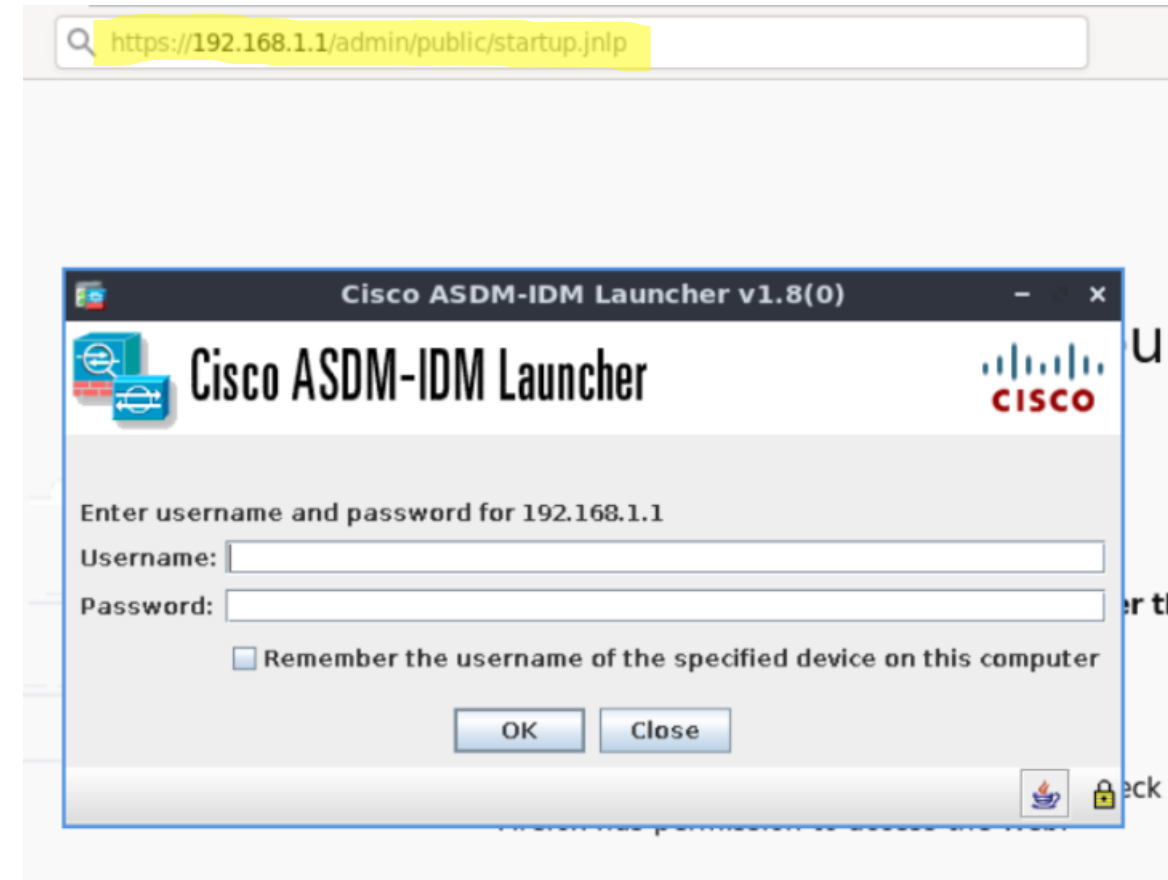
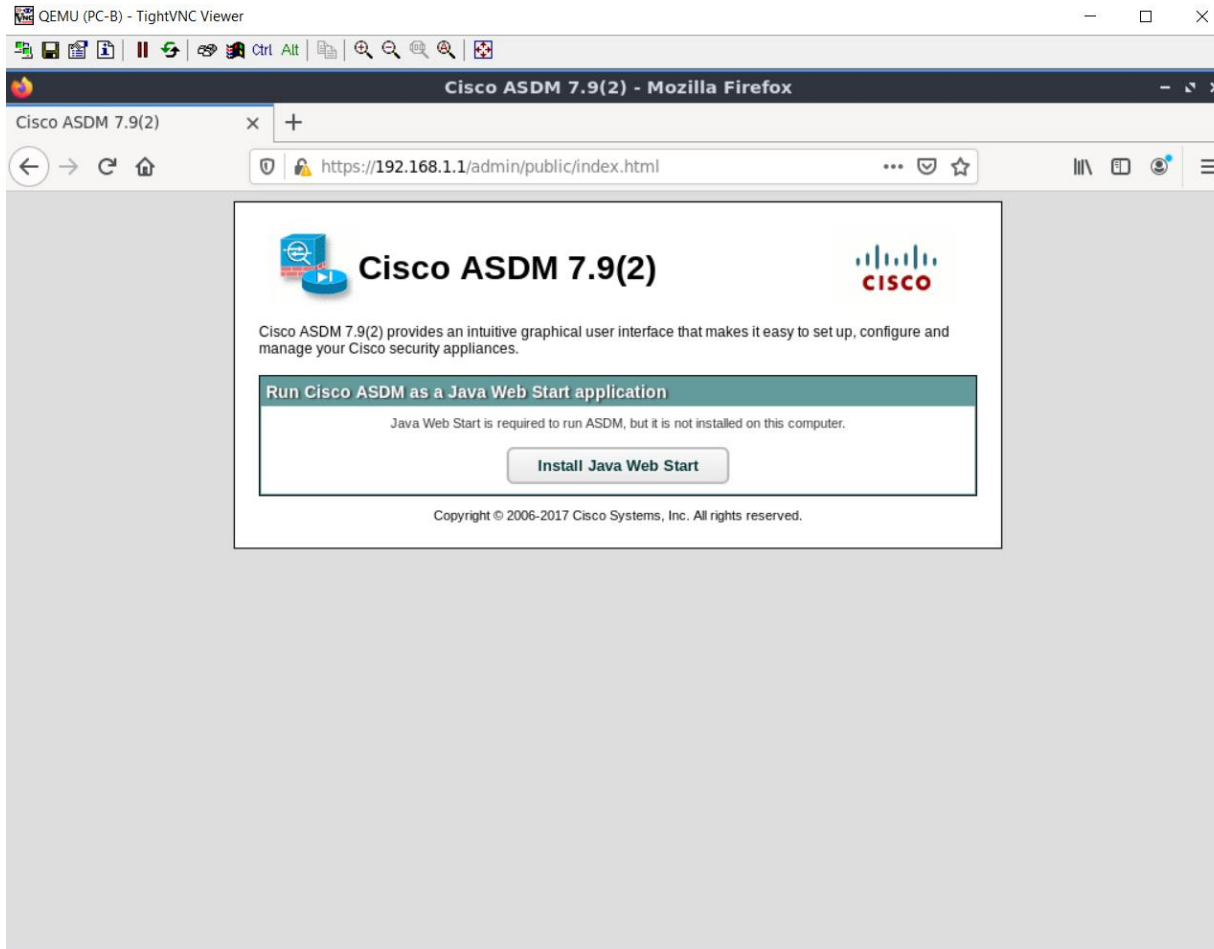
Prístup na ASDM

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



10.1 ASA Security Device Manager (ASDM)

Prístup na ASDM





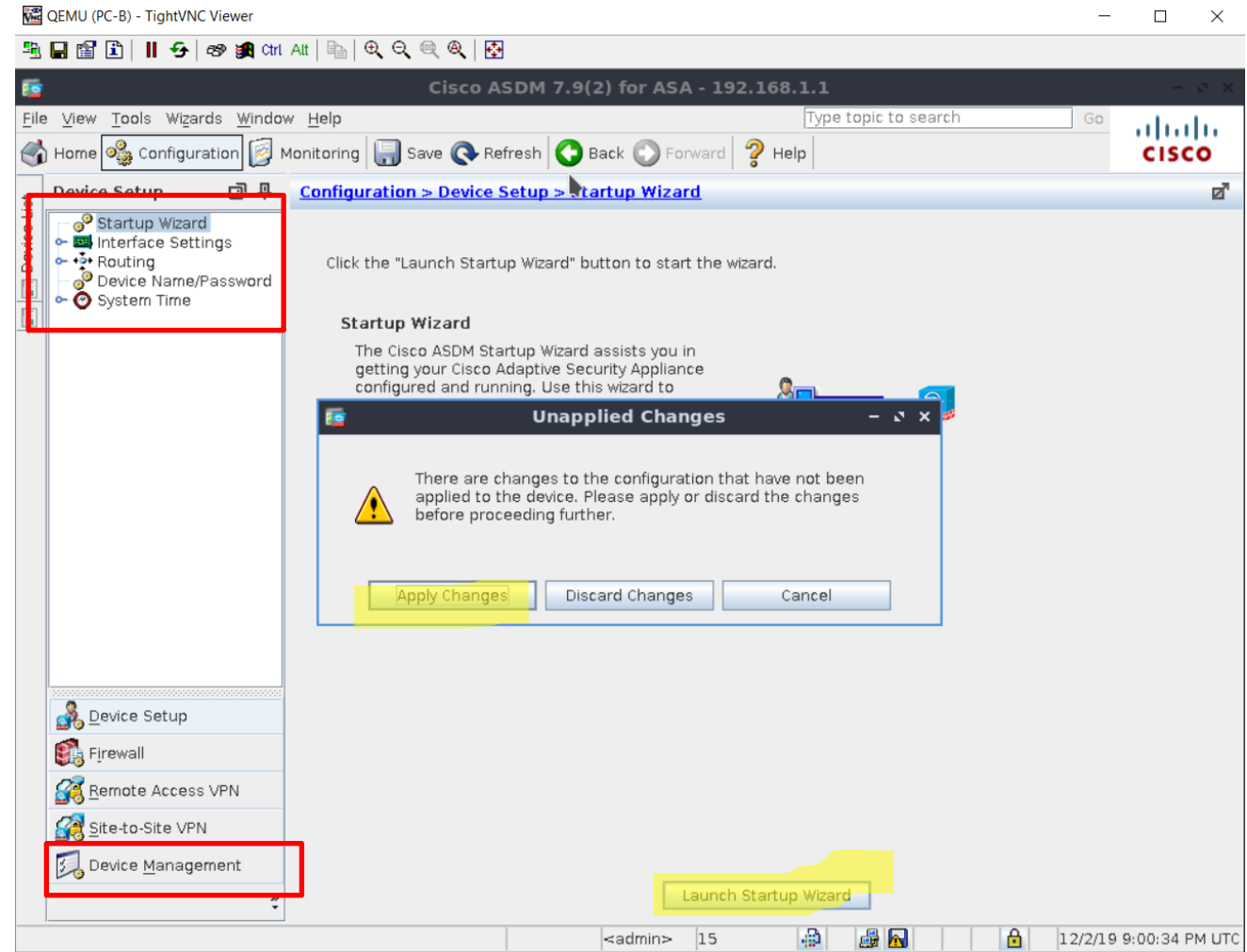
ASDM Security Warning - 1

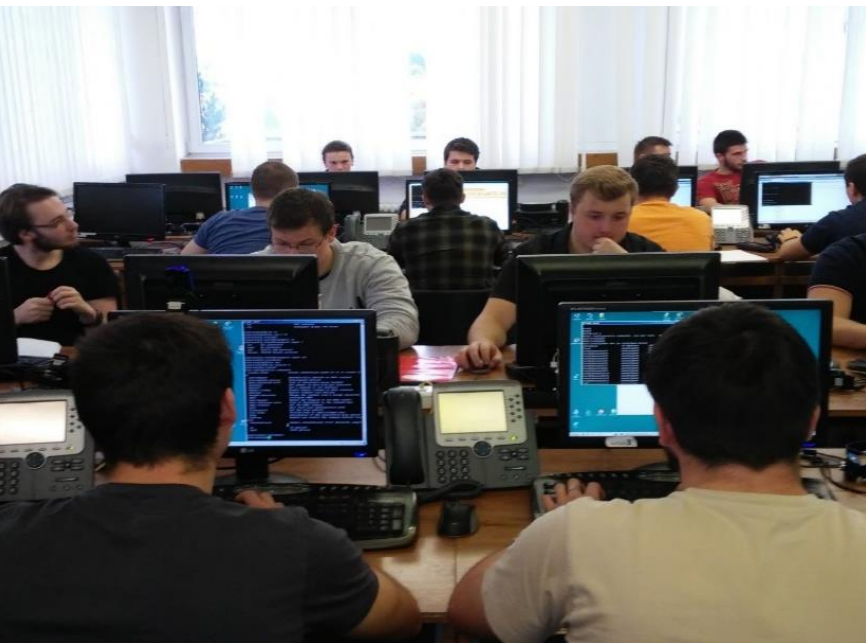
ASDM Security Warning - 2



3. část: Konfigurácia zákl. nastavení ASA cez ASDM

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



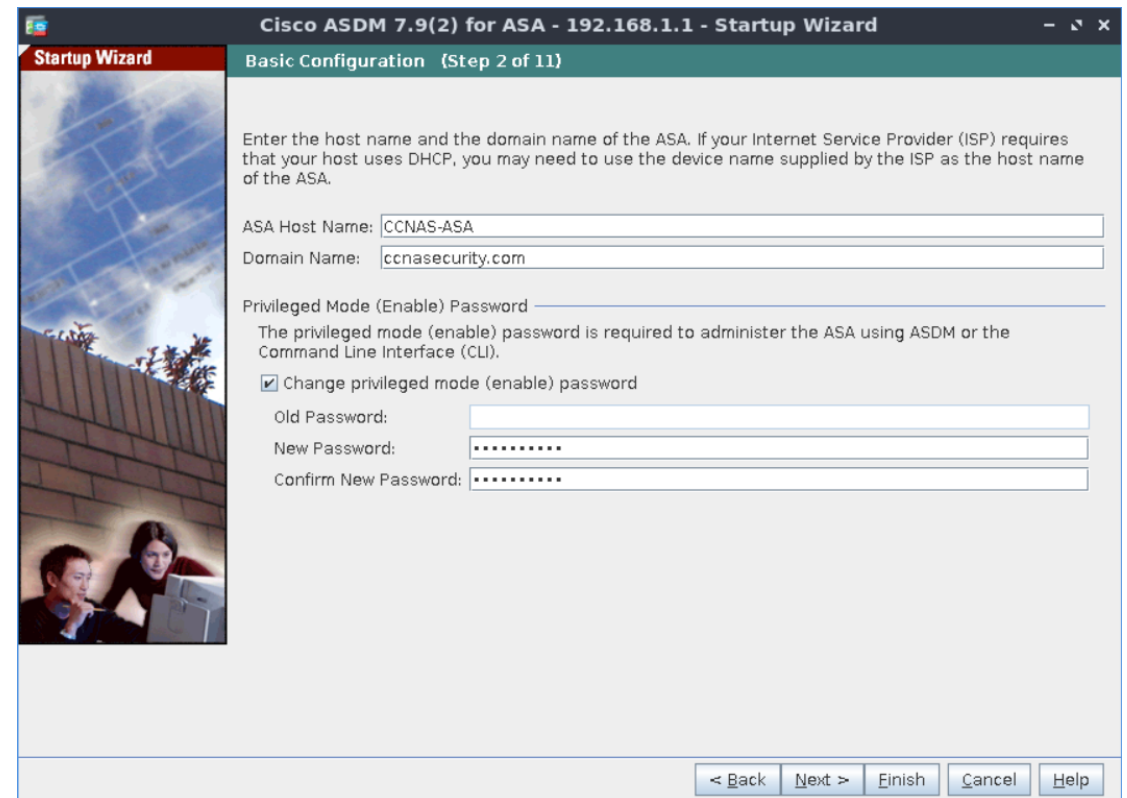
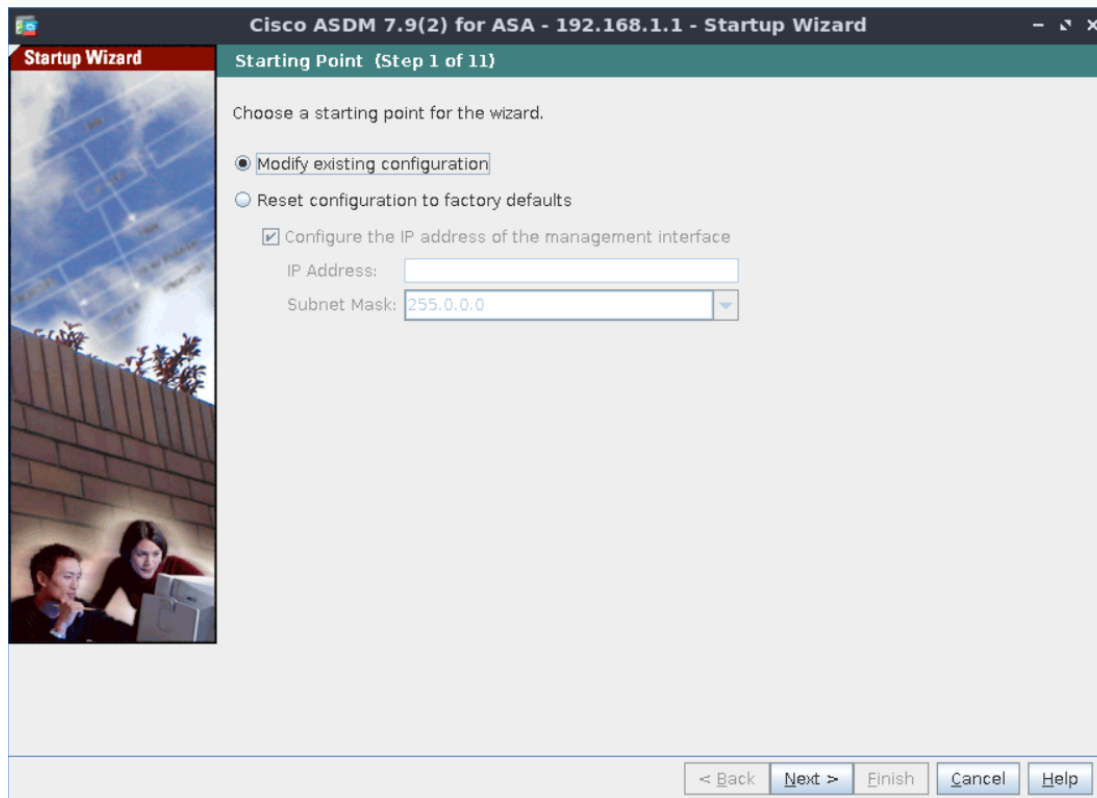


Základná konfigurácia => Wizards

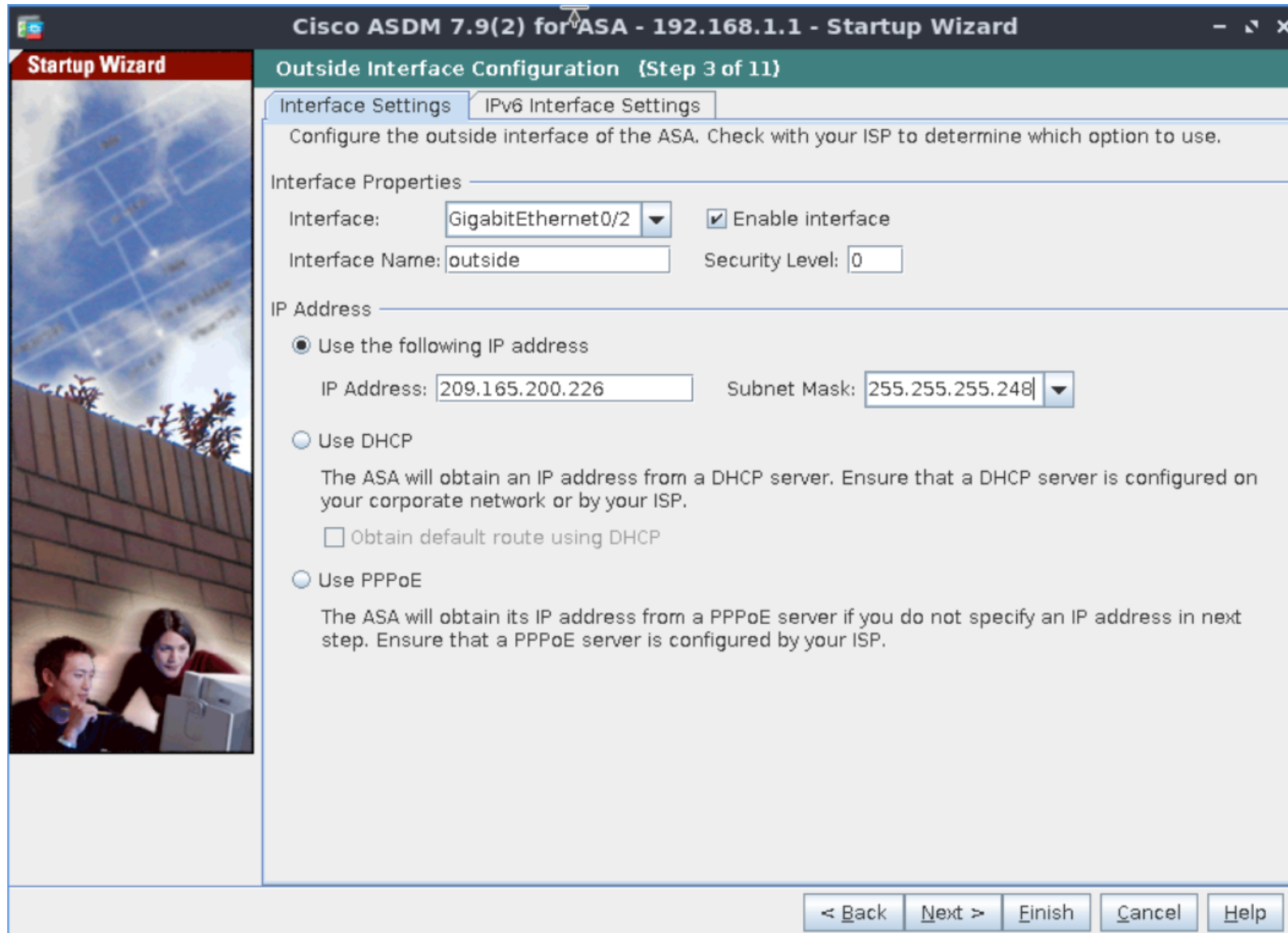
Nastavenie ASA host name, domain name a hesla do privilegovaného módu

Startup Wizard Starting Point Window

Startup Wizard Basic Configuration Window



Konfigurácia vonkajšieho rozhrania



Kontrola vonkajšieho rozhrania

Cisco ASDM 7.9(2) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Other Interface Configuration {Step 4 of 11}

Configure the remaining interfaces of the ASA. To configure an interface, select it in the list below and click Edit.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask/Prefix Length
GigabitEthernet0/0		No			
GigabitEthernet0/1	inside	Yes	100	192.168.1.1	255.255.255.0
GigabitEthernet0/2	outside	Yes	0	209.165.200.226	255.255.255.248
GigabitEthernet0/3		No			
GigabitEthernet0/4		No			
GigabitEthernet0/5		No			
GigabitEthernet0/6		No			
Management0/0		No			

Edit

Enable traffic between two or more interfaces with the same security levels

Enable traffic between two or more hosts connected to the same interface

< Back Next > Finish Cancel Help

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)

Cisco ASDM 7.9(2) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Address Translation (NAT/PAT) (Step 7 of 11)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside interface to the outside interface.

No Address Translation

Use Port Address Translation (PAT)

Use the IP address on the outside interface

Specify an IP address

 IP Address:

Use Network Address Translation (NAT)

 IP Address Range:

< Back Next > Finish Cancel Help

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

Startup Wizard

Startup Wizard Summary (Step 11 of 11)

You have completed the Startup Wizard. To send your changes to the ASA , click Finish. If you want to modify any of the data, click Back.

Configuration Summary:
Host Name: CCNAS-ASA
Domain Name: ccnasecurity.com

Outside interface:
outside (GigabitEthernet0/2), 209.165.200.226

Other named interfaces:
inside (GigabitEthernet0/1), 192.168.1.1

No static routes configured.

DHCP Server is enabled on Inside interface. Pool : 192.168.1.31 - 192.168.1.39

PAT is configured on inside interface.

Administrative access to the device:
HTTPS/ASDM access for 192.168.1.0 through inside
SSH access for 172.16.3.0 through outside
SSH access for 192.168.1.0 through inside

Disable Smart Call Home

< Back Next > Finish Cancel Help

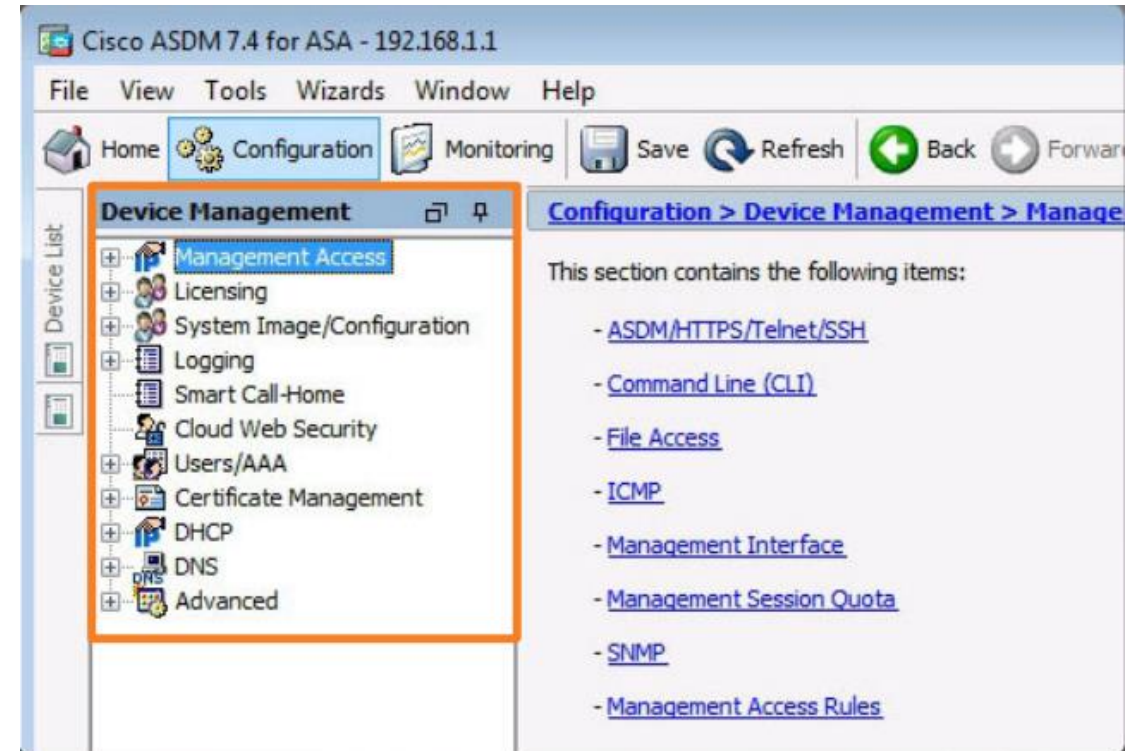
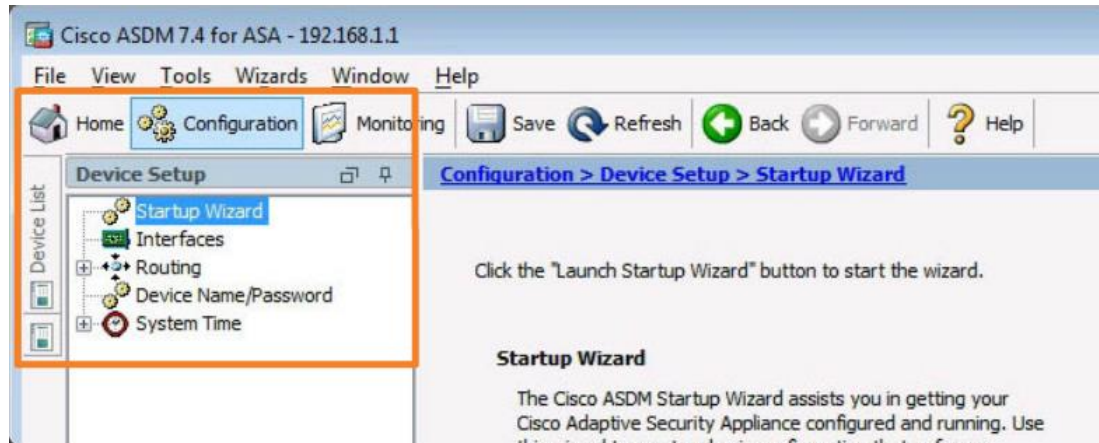


Základná konfigurácia cez ASDM

ASDM – základné nastavenia

Položka Nastavenie zariadenia

Položka Manažment zariadenia



ASDM – základné nastavenia

Configuring Hostname, Domain Name, and Enable Password

Configuring a Master Passphrase

The screenshot shows the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The left sidebar shows the 'Device Setup' tree with 'Device Name/Password' selected. The main content area is titled 'Configuration > Device Setup > Device Name/Password'. It contains the following fields and options:

- Hostname and Domain Name:**
 - Hostname: CCNAS-ASA
 - Domain Name: ccnasecurity.com
- Enable Password:**
 - Change the privileged mode password.
 - Old Password: [empty]
 - New Password: [masked with dots]
 - Confirm New Password: [masked with dots]
- Telnet Password:**
 - Change the password to access the console of the security appliance.
 - Old Password: [empty]
 - New Password: [empty]
 - Confirm New Password: [empty]

The screenshot shows the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The left sidebar shows the 'Device Management' tree with 'Master Passphrase' selected. The main content area is titled 'Configuration > Device Management > Advanced > Master Passphrase'. It contains the following text and fields:

Enable reversible encryption of supported shared keys and passwords. Encryption protects supported shared keys and passwords in the configuration, particularly from viewing while sent insecurely, such as with Telnet.

Encryption occurs when the feature is enabled and the device has a master passphrase. Disabling encryption does not return already encrypted shared keys and passwords to plain text. Only future changes to shared keys and passwords will be in plain text.

Enable Advanced Encryption Standard (AES) password encryption

Passphrase

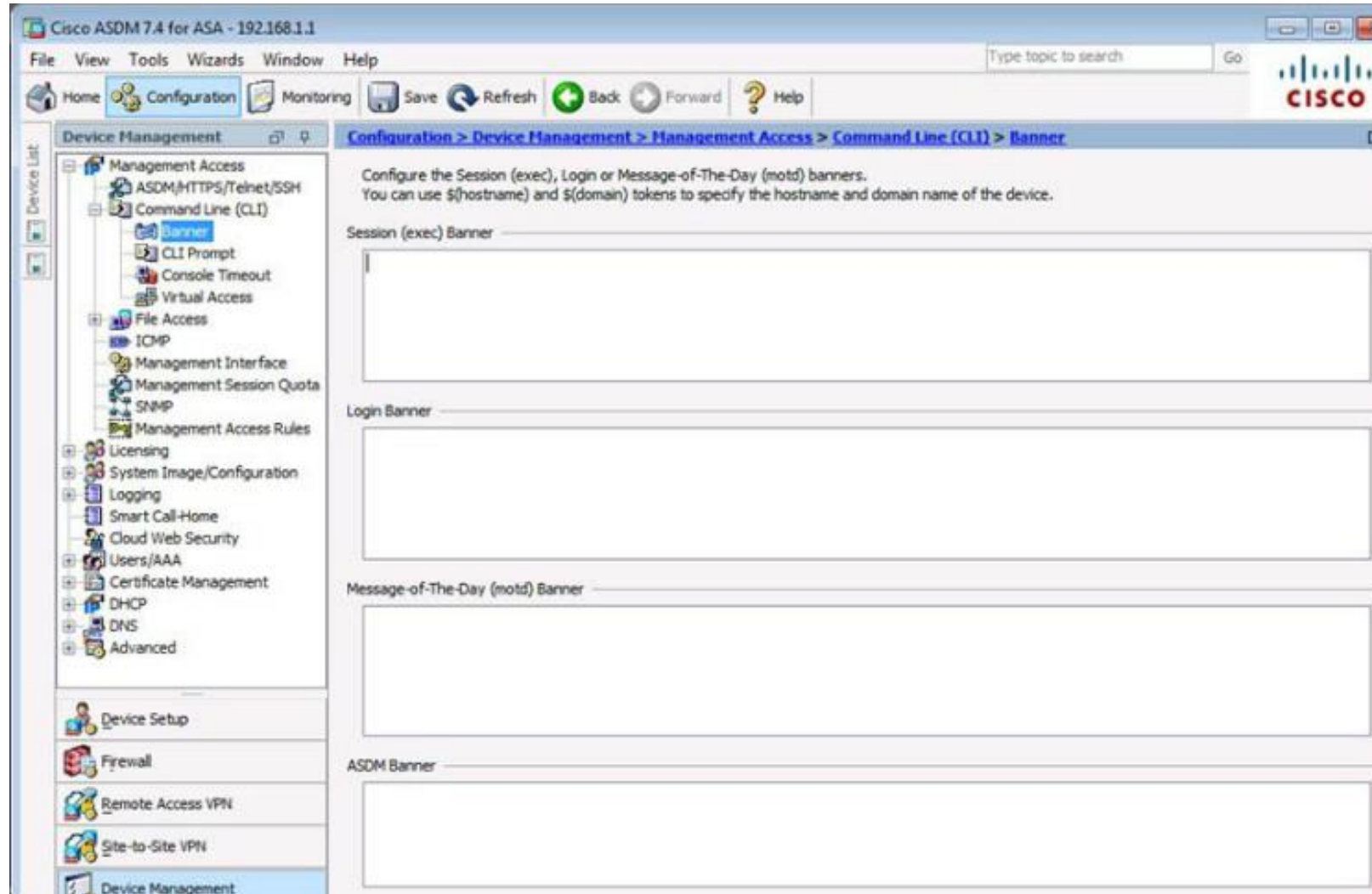
Enter the old master passphrase, if any, and a new master passphrase (8-128 characters) to reversibly encrypt shared keys and passwords. If master passphrase encryption is enabled, encrypts or re-encrypts all supported shared keys and passwords.

To disable encryption and decrypt supported shared keys and passwords, enter the old master passphrase and leave the new passphrase empty.

Change the encryption master passphrase

Old master passphrase: [empty]
New master passphrase: [empty]
Confirm master passphrase: [empty]

ASDM – základné nastavenia - bannery



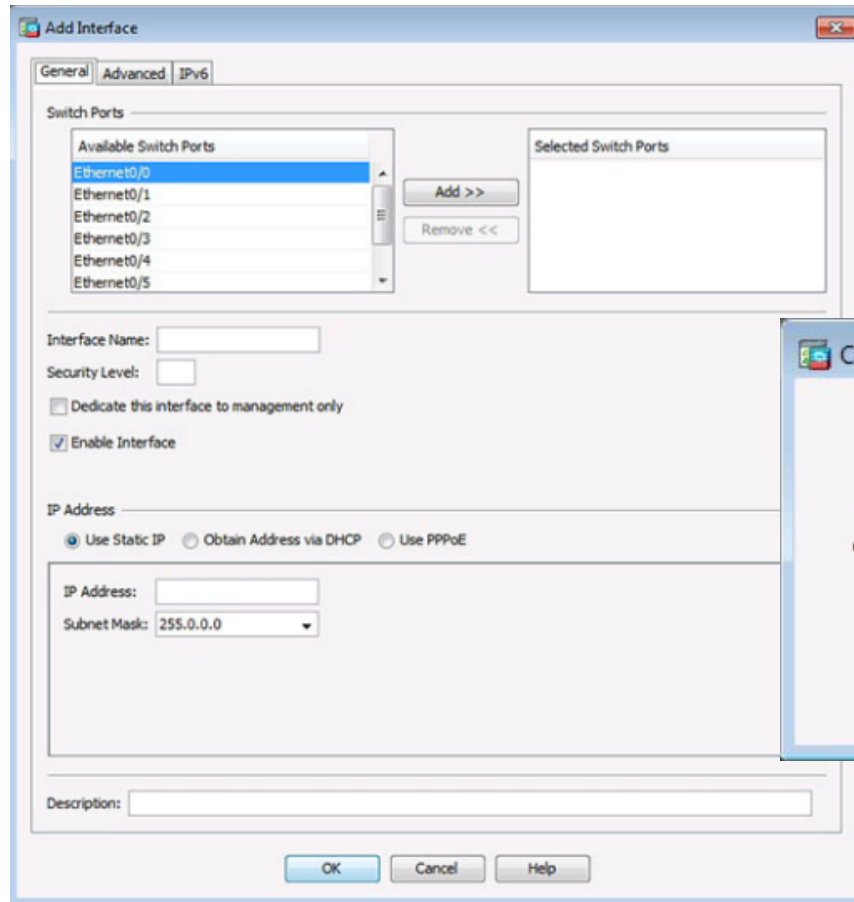
Konfigurácia rozhraní

The screenshot displays the Cisco ASDM 7.4 for ASA configuration interface. The main window title is "Cisco ASDM 7.4 for ASA - 192.168.1.1". The navigation pane on the left shows the "Device Setup" section expanded, with "Interfaces" selected. The main content area shows the "Configuration > Device Setup > Interfaces" page. The "Interfaces" tab is active, displaying a table of configured interfaces. The table has the following columns: Name, Switch Ports, Enabled, Security Level, IP Address, Subnet Mask Prefix Length, and Restrict Traffic flow. A single interface named "inside" is listed with the following details: Switch Ports: Ethernet0/0, Ethernet0/1, Et...; Enabled: Yes; Security Level: 100; IP Address: 192.168.1.1; Subnet Mask Prefix Length: 255.255.255.0. To the right of the table are buttons for "Add", "Edit", and "Delete". Below the table, there are two unchecked checkboxes: "Enable traffic between two or more interfaces which are configured with same security levels" and "Enable traffic between two or more hosts connected to the same interface". At the bottom of the page are "Apply" and "Reset" buttons.

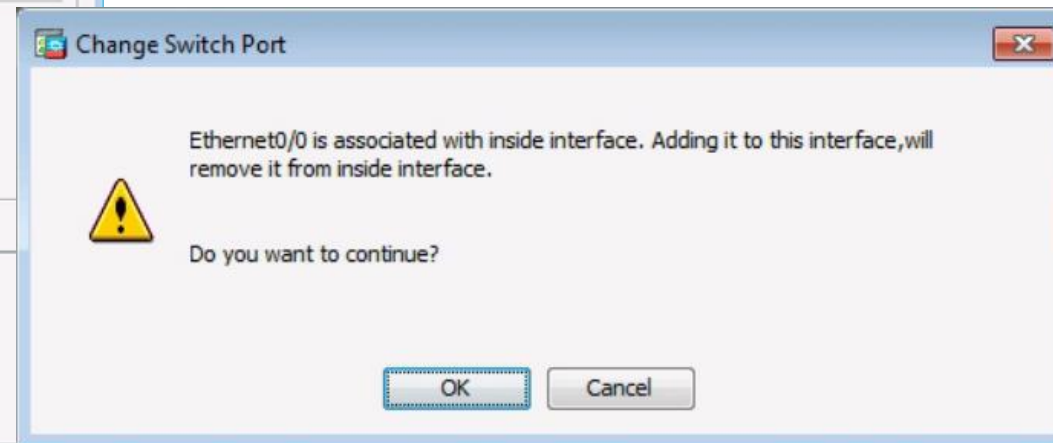
Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/0, Ethernet0/1, Et...	Yes	100	192.168.1.1	255.255.255.0	

Konfigurácia rozhraní

Adding an Outside Interface



Change Switch Port Window



Konfigurácia rozhraní

Adding an Outside Interface

The 'Add Interface' dialog box is shown with the 'General' tab selected. It features three sub-tabs: 'General', 'Advanced', and 'IPv6'. The 'Switch Ports' section contains two lists: 'Available Switch Ports' (Ethernet0/1 through Ethernet0/6) and 'Selected Switch Ports' (Ethernet0/0). Below these are 'Add >>' and 'Remove <<' buttons. The 'Interface Name' is set to 'outside', 'Security Level' is 0, and 'Enable Interface' is checked. The 'IP Address' section has 'Use Static IP' selected, with the IP address '209.165.200.226' and 'Subnet Mask' '255.255.255.248'. A 'Description' field is at the bottom.

Advanced Outside Interface Settings

The 'Add Interface' dialog box is shown with the 'Advanced' tab selected. It features three sub-tabs: 'General', 'Advanced', and 'IPv6'. The 'MTU' is set to 1500 and 'VLAN ID' is set to 2. The 'MAC Address Cloning' section has a text area for instructions and two input fields for 'Active MAC Address' and 'Standby MAC Address'. The 'Block Traffic' section has a dropdown menu for 'Block traffic from this interface to:'.

Updated Interface Page

Configuration > Device Setup > Interfaces



Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow	
inside	Ethernet0/0, Ethernet0/1, Et...	Yes	100	192.168.1.1	255.255.255.0		Add
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248		Edit
							Delete

Konfigurácia rozhraní

Verifying Interfaces

Configuration > Device Setup > Interfaces

Interfaces Switch Ports

Switch Port	Enabled	Associated VLANs	Associated Interface Names	Mode	Protected	Duplex	Speed	Edit
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

Switch Port: Ethernet0/0 Enable SwitchPort

Mode and VLAN IDs

Access
VLAN ID: 2

Trunk
VLAN IDs:

Configure Native VLAN Native VLAN ID:

VLAN ID must be in the range of 1 to 4090. For access mode, only one VLAN ID is allowed. For trunk mode, up to 20 comma-separated VLAN IDs can be entered.

Isolated

Isolated
An isolated/protected port does not forward any traffic to any other isolated port within the same VLAN

Dupl... auto Speed: auto

OK Cancel Help

Enable Switch Ports

Apply
Configuration

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/1, Ethernet0/2, Et...	Yes	100	192.168.1.1	255.255.255.0	
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248	

Add Edit Delete

10.1 ASA Security Device Manager (ASDM)

Overenie stavu rozhraní

The screenshot shows the Cisco ASDM 7.9(2) interface for ASA - 192.168.1.1. The 'Interface Status' table is highlighted, showing the following data:

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	2
outside	209.165.200.226...	up	up	0

The 'Traffic Status' section shows 'Connections Per Second Usage' and 'outside' Interface Traffic Usage (Kbps) graphs. The status bar at the bottom indicates the user is <admin> and the time is 12/2/19 10:06:04 PM UTC.

The screenshot shows the Cisco ASDM 7.9(2) interface for ASA - 192.168.1.1. The 'Interface Status' table is highlighted, showing the following data:

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	3
outside	209.165.200.226...	up	up	0

The 'Traffic Status' section shows 'Connections Per Second Usage' and 'outside' Interface Traffic Usage (Kbps) graphs. A yellow highlight is present on the 'outside' Interface Traffic Usage graph. The status bar at the bottom indicates the user is <admin> and the time is 12/2/19 10:10:54 PM UTC.

Konfigurácia HTTPS/Telnet/SSH

The screenshot shows the Cisco ASDM 7.4 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH. The main content area is titled "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH." It contains a table with the following data:

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	192.168.1.3	255.255.255.255

Below the table are sections for "Http Settings", "Telnet Settings", and "SSH Settings".

Http Settings:

- Enable HTTP Server
- Port Number: 443
- Idle Timeout: 20 minutes
- Session Timeout: minutes
- Require client certificate to access ASDM on the following interfaces: Interfaces: (dropdown menu)

Telnet Settings:

- Telnet Timeout: 5 minutes

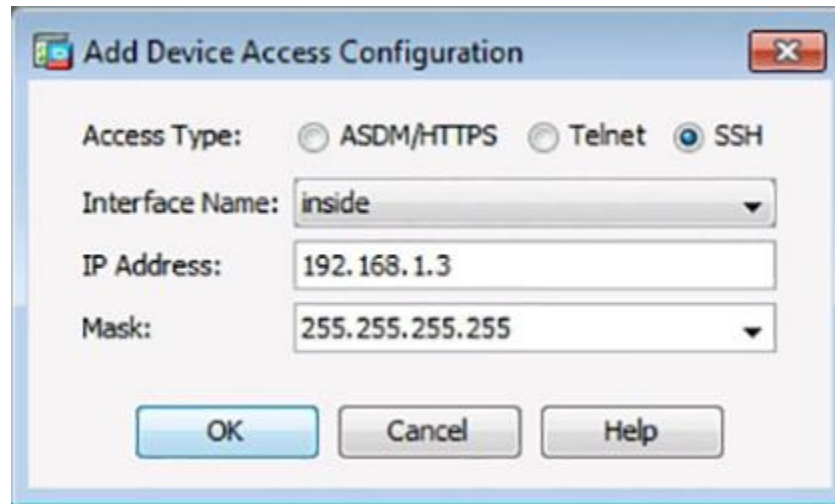
SSH Settings:

- Allowed SSH Version(s): 1 & 2
- SSH Timeout: 5 minutes
- DH Key Exchange: Group 1 Group 14

Buttons for "Apply" and "Reset" are at the bottom. The status bar shows <admin> | 15 | 4/14/15 1:15:21 PM EDT.

SSH

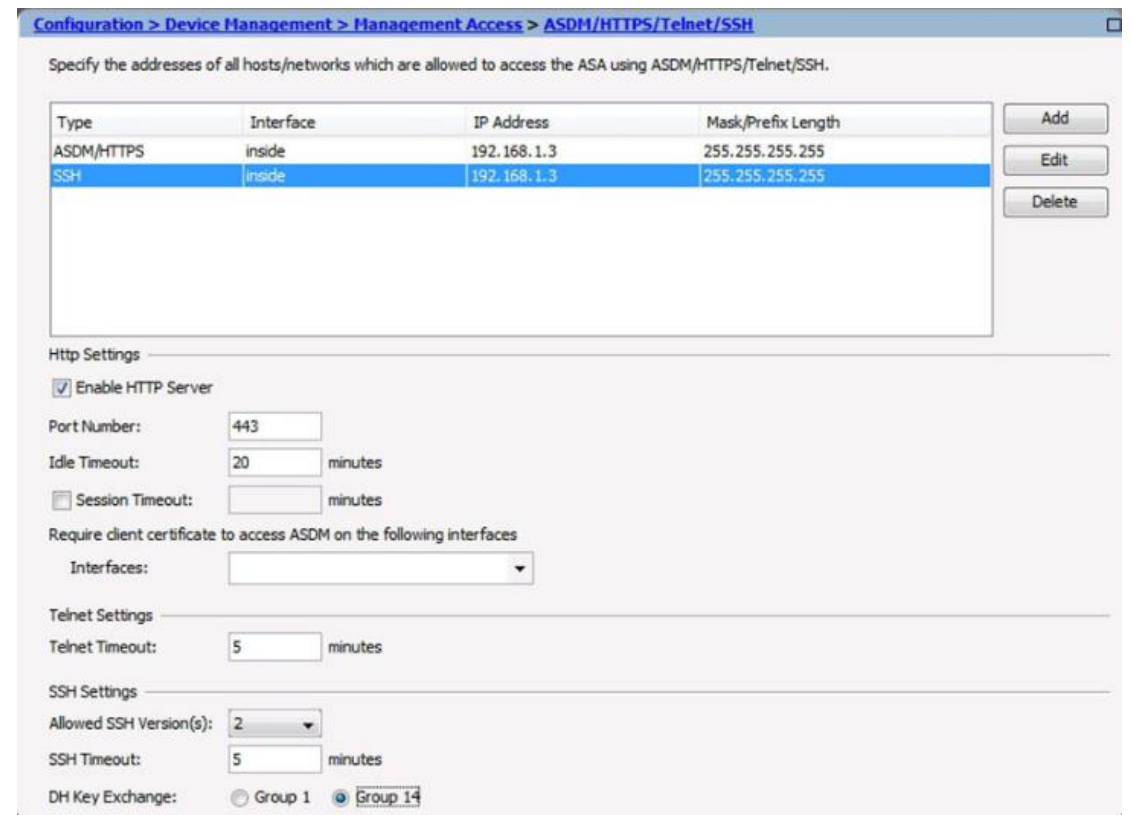
Add Device Access Configuration Window



The dialog box titled "Add Device Access Configuration" has a close button (X) in the top right corner. It contains the following fields and controls:

- Access Type:** Three radio buttons: ASDM/HTTPS, Telnet, and SSH.
- Interface Name:** A dropdown menu with "inside" selected.
- IP Address:** A text input field containing "192.168.1.3".
- Mask:** A dropdown menu with "255.255.255.255" selected.
- At the bottom, there are three buttons: "OK", "Cancel", and "Help".

Configure SSH Settings



The configuration page is titled "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". It includes a breadcrumb trail and a close button. The main content area is titled "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH." and contains a table with the following data:

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	192.168.1.3	255.255.255.255
SSH	inside	192.168.1.3	255.255.255.255

Buttons for "Add", "Edit", and "Delete" are located to the right of the table. Below the table are several sections of settings:

- Http Settings:** Includes a checked checkbox for "Enable HTTP Server", a "Port Number" field set to 443, an "Idle Timeout" field set to 20 minutes, and an unchecked checkbox for "Session Timeout".
- Require client certificate to access ASDM on the following interfaces:** Includes an "Interfaces:" dropdown menu.
- Telnet Settings:** Includes a "Telnet Timeout" field set to 5 minutes.
- SSH Settings:** Includes an "Allowed SSH Version(s)" dropdown set to 2, an "SSH Timeout" field set to 5 minutes, and a "DH Key Exchange" section with radio buttons for "Group 1" and "Group 14" (which is selected).

Otestovanie HTTP pripojenia cez Packet Tracer

The screenshot shows the Cisco ASDM Packet Tracer interface. The main window is titled "Cisco ASDM Packet Tracer - 192.168.1.1". The interface includes a menu bar, a toolbar, and a main workspace. The workspace is divided into several sections:

- Configuration Section:** A form for setting packet parameters. The "Interface" is set to "inside". The "Packet Type" is set to "TCP". The "Source" is "IP Address" with value "192.168.1.3". The "Destination" is "IP Address" with value "209.165.200.225". The "Source Port" is "1500" and the "Destination Port" is "http". There are "Start" and "Clear" buttons.
- Show animation:** A checkbox that is checked, indicating that the packet flow is being visualized.
- Flow Diagram:** A horizontal sequence of icons representing the packet's path through various network layers and protocols. From left to right, the icons are: "inside", "QOS", "NAT Lookup", "QOS", "NAT Lookup", "IP Options Lookup", "Flow creation", "Route Lookup", "ADJACENCY", and "UNKNO...". Each icon has a green checkmark above it, indicating successful completion of that phase.
- Phase List:** A table-like view showing the sequence of phases the packet went through. Each phase has a green checkmark in the "Acti..." column, indicating success.

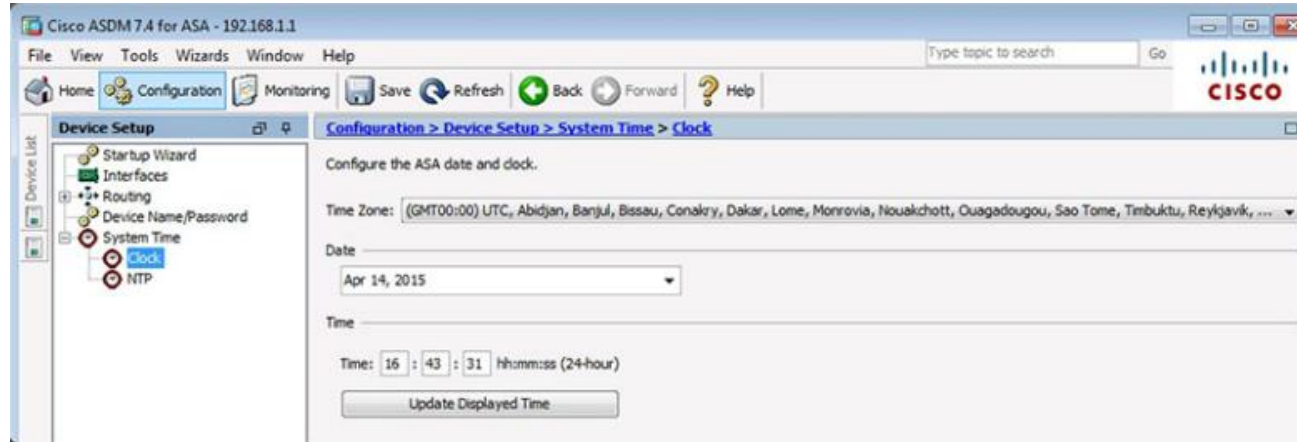
Phase	Acti...
ACCESS-LIST	✓
ROUTE-LOOKUP	✓
NAT	✓
NAT	✓
IP-OPTIONS	✓
QOS	✓
NAT	✓
QOS	✓
NAT	✓
IP-OPTIONS	✓
FLOW-CREATION	✓
ROUTE-LOOKUP	✓
ADJACENCY-LOOKUP	✓
RESULT - The packet is allowed.	✓



Konfigurácia ďalších nastavení ASA cez ASDM

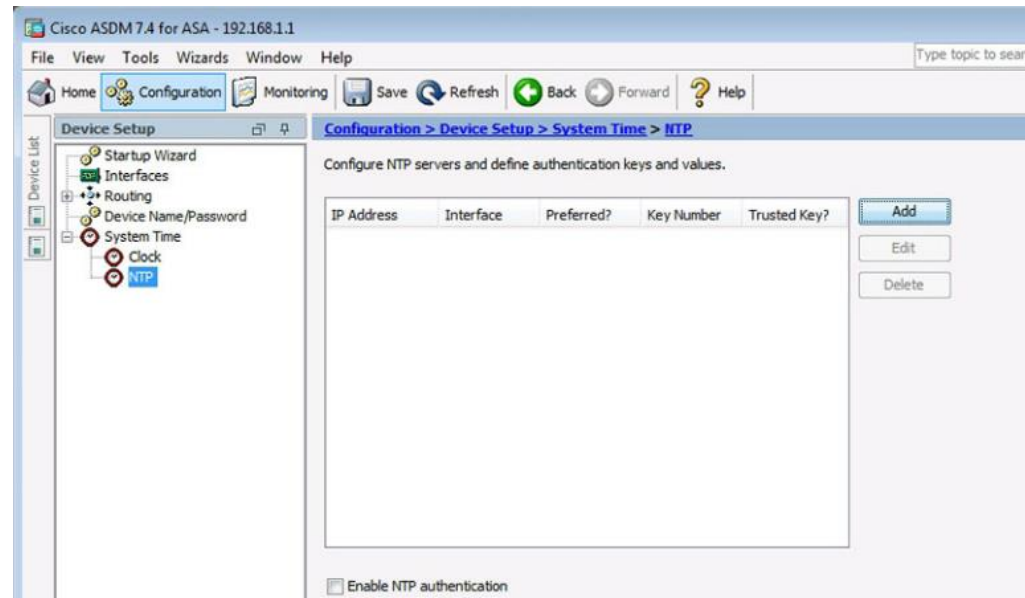
Konfigurácia času

Nastavenie času

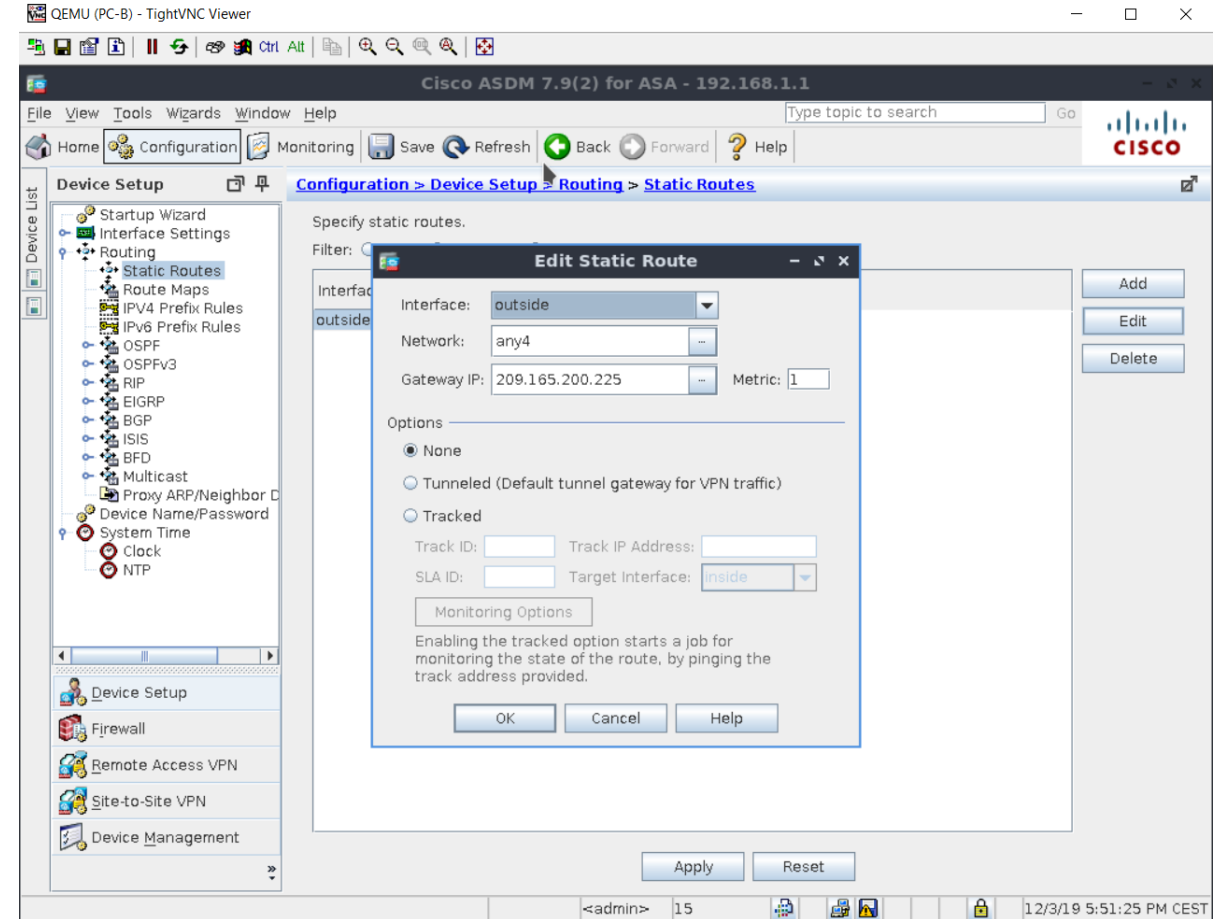
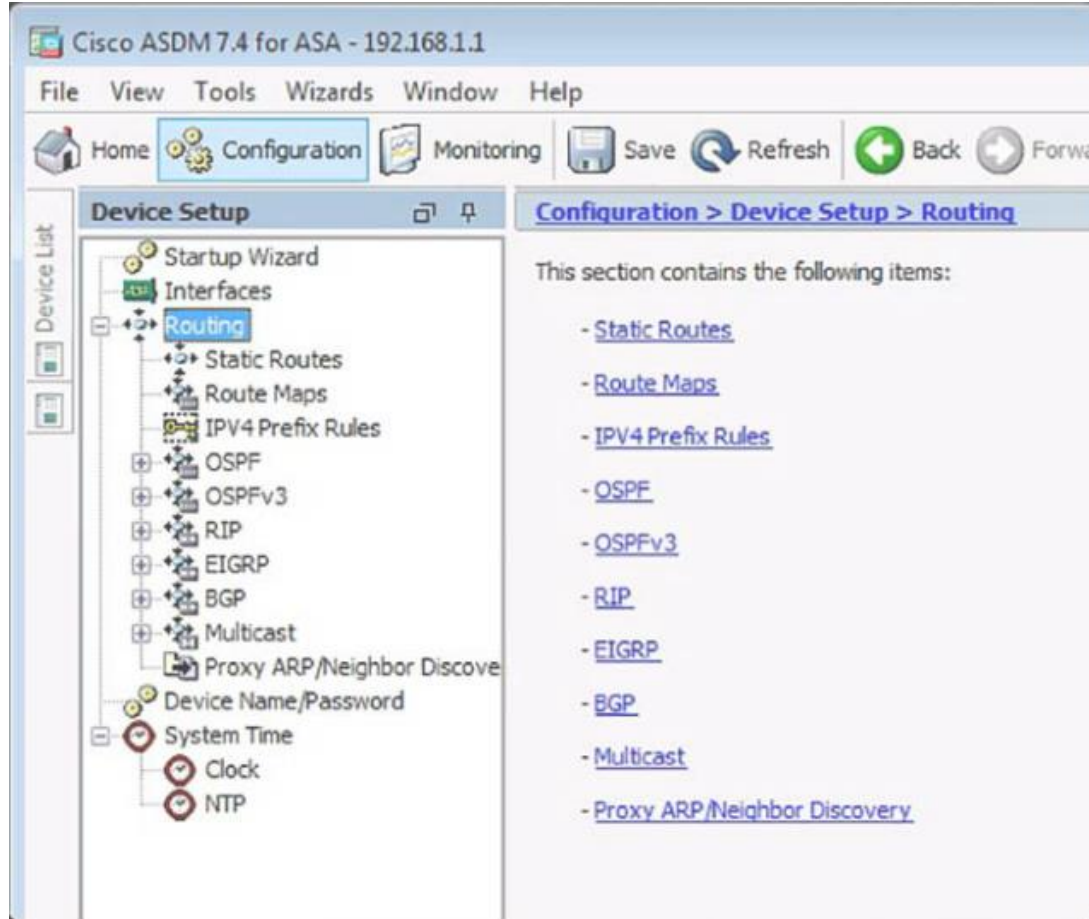


Manually Change
the System Time

Use NTP to Change the
System Time



Konfigurácia predvolenej statickej cesty



Nezabudni na vždy Apply

Configuration > Device Setup > Routing > Static Routes

Specify static routes.

Filter: Both IPv4 only IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
outside	0.0.0.0	255.255.25...	209.165.2...	1	None

Add
Edit
Delete

Overenie funkčnosti predvolenej statickej cesty

The screenshot displays the Cisco ASDM 7.9(2) for ASA - 192.168.1.1 interface. The main window is titled "Ping" and is used for testing network connectivity. The configuration is as follows:

- Packet Type:** ICMP, TCP
- Destination:** IP Address or Hostname: 10.1.1.1, Port: (empty)
- Source:** Interface (optional): -- None --, IP Address (optional): (empty)
- Port:** Random port, Starting port: (empty)
- Repeat(optional):** (empty), **Timeout(optional):** (empty)

The **Ping Output** section shows the following results:

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/10 ms
```

The interface also includes buttons for "Add", "Edit", "Delete", "Ping", "Close", "Help", "Clear Output", "Apply", and "Reset". The status bar at the bottom indicates "Configuration changes saved successfully." and shows the user as <admin> with 15 sessions. The system time is 12/3/19 5:53:55 PM CEST.

Traceroute ASA → PC-C

QEMU (PC-B) - TightVNC Viewer

Cisco ASDM 7.9(2) for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Routing > Static Routes

Device List

- Startup Wizard
- Interface Settings
- Routing
 - Static Routes
 - Route Maps
 - IPV4 Prefix Lists
 - IPV6 Prefix Lists
 - OSPF
 - OSPFv3
 - RIP
 - EIGRP
 - BGP
 - ISIS
 - BFD
 - Multicast
 - Proxy ARP
- Device Name
- System Time
- Clock
- NTP

Device Setup

Firewall

Remote Access

Site-to-Site VPN

Device Management

Traceroute

Host Name or IP Address: 172.16.3.3

Optional Parameters

Timeout: [] (default: 3 sec) Specify source interface or IP address

Port: [] (default: 33434) Source Interface Source IP []

Probe: [] (default: 3) Reverse resolve Use ICMP

Min. & Max. TTL: [] [] (defaults: 1 and 30)

Traceroute Output

Type escape sequence to abort.

Tracing the route to 172.16.3.3

```
1 209.165.200.225 8 msec 10 msec 10 msec
2 10.1.1.2 40 msec 20 msec 24 msec
3 10.2.2.1 56 msec 60 msec 40 msec
4 172.16.3.3 101 msec 50 msec 50 msec
```

Clear Output

Trace Route Close Help

Apply Reset

Configuration changes saved successfully. <admin> 15 12/3/19 5:55:45 PM CEST

Konfigurácia DHCP služby

The screenshot shows the Cisco ASDM 7.4 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > DHCP > DHCP Server. The left sidebar shows the configuration tree with 'DHCP Server' selected. The main area displays a table of DHCP server configurations for interfaces 'inside' and 'outside'. Below the table are sections for 'Global DHCP Options' and 'Dynamic DNS Settings for DHCP Server'.

Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout
inside	No	-				
outside	No	-				

Global DHCP Options

Enable auto-configuration from interface: outside Allow VPN override

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

DNS Server 1: Primary WINS Server:
DNS Server 2: Secondary WINS Server:
Domain Name:
Lease Length: secs
Ping Timeout: ms

Dynamic DNS Settings for DHCP Server

Update DNS Server

Update Both Records Override Client Settings

Konfigurácia DHCP služby

Edit DHCP Server Window

Interface: **inside**

Enable DHCP server

DHCP Address Pool: -

Optional Parameters

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Lease Length: seconds Ping Timeout: milliseconds

Domain Name:

Auto-Configuration

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

Enable auto-configuration from interface: Allow VPN override

Advanced Options

Advanced Parameters :

Dynamic DNS Settings for DHCP Server

Update DNS server

Update both records Override client settings

Configuring DHCP Server Services

Interface: **inside**

Enable DHCP server

DHCP Address Pool: -

Optional Parameters

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Lease Length: seconds Ping Timeout: milliseconds

Domain Name:

Auto-Configuration

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

Enable auto-configuration from interface: Allow VPN override

Advanced Options

Advanced Parameters :

Dynamic DNS Settings for DHCP Server

Update DNS server

Update both records Override client settings

Konfigurácia AAA s využívaním lokálnej DB ASA

The screenshot displays the Cisco ASDM 7.9(2) for ASA - 192.168.1.1 interface. The left pane shows the navigation tree with 'Users/AAA' expanded to 'User Accounts'. The main pane shows the 'Add User Account' configuration page. The 'Identity' section is selected, and the 'Add' button is visible. The 'Access Restriction' section is also visible, with 'Full access(ASDM, SSH, Telnet and Console)' selected. The 'Privilege Level' is set to 15.

Configuration page: **Add User Account**

Identity:

- Public Key Authentic
- Public Key Using PKF
- VPN Policy

Username: admin01

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 15

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if "aaa authentication http console LOCAL" command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are con

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
enable_15	15	Full	N/A	N/A

Find:

Apply Reset

<admin> 15 12/3/19 6:02:45 PM CEST

Overenie DHCP služby

Configuration > Device Management > DHCP > DHCP Server

Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout	Edit
inside	Yes	192.168.1.10 - 192.168.1.41			ccnasecurity....		
outside	No	-					

Global DHCP Options

Enable auto-configuration from interface: outside Allow VPN override

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Domain Name:

Lease Length: secs

Ping Timeout: ms

Dynamic DNS Settings for DHCP Server

Update DNS Server

Update Both Records Override Client Settings

Konfigurácia AAA s využívaním lokálnej DB ASA

The screenshot displays the Cisco ASDM 7.9(2) for ASA - 192.168.1.1 interface. The breadcrumb navigation path is Configuration > Device Management > Users/AAA > AAA Access > Authentication. The left sidebar shows the Device Management tree with 'Users/AAA' expanded to 'AAA Access'. The main content area shows the 'Authentication' configuration page with the following settings:

- Enable authentication for administrator access to the ASA. Enable
- Require authentication to allow use of privileged mode commands: Enable
- Require authentication for the following types of connections:
 - HTTP/ASDM: Use LOCAL when server group fails
 - Serial: Use LOCAL when server group fails
 - SSH: Use LOCAL when server group fails
 - Telnet: Use LOCAL when server group fails

Buttons for 'Apply' and 'Reset' are visible at the bottom. The status bar at the bottom indicates 'Configuration changes saved successfully.' and shows the user as '<admin>' with 15 sessions. The system time is 12/3/19 6:07:55 PM CEST.

Vygenerovanie RSA kľúča

QEMU (PC-B) - TightVNC Viewer

Cisco ASDM 7.9(2) for ASA - 192.168.1.1

Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: ASDM_TrustPoint0

Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From: Browse...

Add a new identity certificate:

Key Pair: <Default-RSA-Key> Show... New...

Certificate Subject DN: CN=CCNAS-ASA Select...

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

Add Certificate Cancel Help

Identity Certificate Request

To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

Save CSR to File: kluč Browse...

OK Cancel Help

Enable CA flag in basic constraints extension

Add Certificate Cancel Help

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

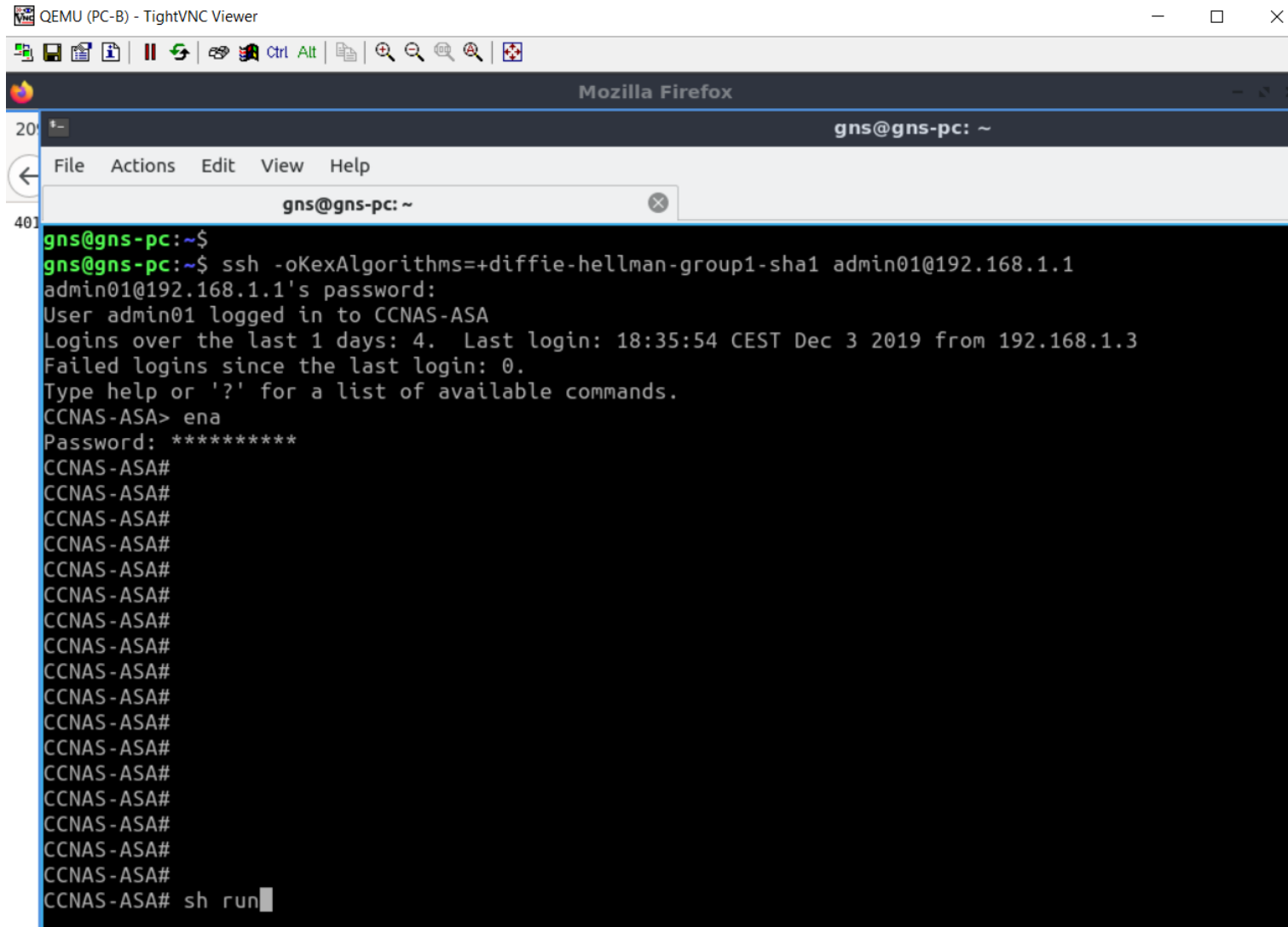
Enroll ASA SSL certificate with Entrust

Using a previously saved certificate signing request, [enroll with Entrust](#).

Apply Reset

Configuration changes saved successfully. <admin> 15 12/3/19 6:30:05 PM CEST

Otestovanie SSH prístupu na ASA



The image shows a terminal window titled "QEMU (PC-B) - TightVNC Viewer" running Mozilla Firefox. The terminal session is as follows:

```
gns@gns-pc: ~  
gns@gns-pc:~$ ssh -oKexAlgorithms+=diffie-hellman-group1-sha1 admin01@192.168.1.1  
admin01@192.168.1.1's password:  
User admin01 logged in to CCNAS-ASA  
Logins over the last 1 days: 4. Last login: 18:35:54 CEST Dec 3 2019 from 192.168.1.3  
Failed logins since the last login: 0.  
Type help or '?' for a list of available commands.  
CCNAS-ASA> ena  
Password: *****  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA#  
CCNAS-ASA# sh run
```

Cisco Modular Policy Framework (MPF)

The screenshot displays the Cisco ASDM 7.9(2) for ASA - 192.168.1.1 interface. The main window shows the configuration of a Service Policy Rule. The 'Edit Service Policy Rule' dialog is open, showing the 'Protocol Inspection' tab. The 'Protocol Inspection' tab is active, and the 'Select all inspection rules' checkbox is unchecked. The following protocols are checked:

- DNS
- ESMTMP
- FTP
- H.323 H.225
- H.323 RAS
- ICMP
- IP-Options

The 'DNS' protocol is configured with the 'DNS Inspect Map: migrated_dns_map_1'. The 'ICMP' protocol is highlighted in yellow. The 'Edit Service Policy Rule' dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

5. časť: Konfigurácia DMZ, statického NAT a ACL

The screenshot displays the Cisco ASDM configuration interface for a Cisco ASA device. The main window is titled "Configuration > Device Setup > Interface Settings > Interface Settings". A table lists the interfaces:

Interface	Name	Zone	Route
GigabitEthernet0/0			
GigabitEthernet0/1	inside		
GigabitEthernet0/2	outside		
GigabitEthernet0/3			
GigabitEthernet0/4			
GigabitEthernet0/5			
GigabitEthernet0/6			
Management0/0			

The "dmz" interface configuration window is open, showing the following settings:

- Hardware Port: GigabitEthernet0/0
- Bridge Group: --None--
- Interface Name: dmz
- Zone: --None--
- Route Map: --None--
- Security Level: 70
- Threat Detection is enabled (indicated by a red X icon).
- Options: Dedicate this interface to management only, VTEP source interface, Enable Interface.
- IP Address: Use Static IP, Obtain Address via DHCP, Use PPPoE.
- IP Address: 192.168.2.1
- Subnet Mask: 255.255.255.0
- Description: (empty field)

Navigation buttons (OK, Cancel, Help) are visible at the bottom of the configuration window.

Overenie konfigurácie DMZ rozhrania

The screenshot shows the Cisco ASDM configuration page for 'Configuration > Device Setup > Interface Settings > Interfaces'. The interface configuration table is as follows:

Interface	Name	Zone	Route Map	State	Security Level	IP Address
GigabitEthernet0/0	dmz			Enabled	70	192.168.2.1
GigabitEthernet0/1	inside			Enabled	100	192.168.1.1
GigabitEthernet0/2	outside			Enabled	0	209.165.200.226
GigabitEthernet0/3				Disabl...		
GigabitEthernet0/4				Disabl...		
GigabitEthernet0/5				Disabl...		
GigabitEthernet0/6				Disabl...		
Management0/0				Disabl...		

Below the table, the following options are visible:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface
- Enable jumbo frame reservation
- Enable auto-generation of MAC addresses for subinterfaces

Prefix: (if you do not enter a prefix, the ASA will generate one for you.)

Buttons: Apply, Reset

Konfigurácia DMZ servera

The screenshot displays the Cisco ASDM (ASA Security Device Manager) interface. The main window is titled "Configuration > Firewall > Public Servers". The left sidebar shows a "Device List" with various configuration categories like "Access Rules", "NAT Rules", "Service Policy Rules", "AAA Rules", "Filter Rules", "Ethertype Rules", "Public Servers", "URL Filtering S", "Threat Detect", "Identity Option", "Identity by Tru", "VM Attribute A", "Botnet Traffic", "Objects", "Unified Commu", and "Advanced". The "Public Servers" category is selected. The main content area contains a description: "Define the servers and services that you would like to expose to an outside interface." Below this, there are tabs for "Private Interface", "Private IP Address", "Private Service", "Public Interface", "Public IP Address", and "Public Service". The "Public Interface" tab is active, showing a dropdown menu with "outside" selected. Other fields include "Private Interface" (dmz), "Private IP Address" (empty), "Private Service" (empty), and "Public IP Address" (209.165.200.227). There are "Add", "Edit", and "Delete" buttons on the right. A modal dialog box titled "Add Public Server" is open in the foreground, providing instructions: "Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface, address of the server, and the service to be exposed. Finally, specify the public interface, address, and service in which the server will be seen." The dialog contains the same fields as the main window, with "Specify Public Service if different from Private Service. This will enable the static PAT." checkbox and a "Public Service" dropdown (TCP or UDP service only). "OK", "Cancel", and "Help" buttons are at the bottom of the dialog. The bottom of the ASDM window shows "Apply" and "Reset" buttons, and a status bar with "admin01", "15", and a timestamp "12/3/19 7:17:15 PM CES".

Konfigurácia DMZ servera

The screenshot displays the ASDM configuration interface for a Cisco ASA. The main window is titled "Browse Private IP Address" and shows a table of network objects. A dialog box titled "Add Network Object" is open, showing the configuration for a new object named "DMZ-Server".

Add Network Object Dialog:

- Name: DMZ-Server
- Type: Host
- IP Version: IPv4 IPv6
- IP Address: 192.168.2.3
- Description: PC-A
- NAT: (checkbox)

Browse Private IP Address Window:

Name	IP Address	Netmask	Description	Object NAT Add...	Agent Name	Attribute Type	Attribute V...
Network Objects							
DMZ-Server	192.168.2.3		PC-A				





















Selected Private IP Address: DMZ-Server

Povolenie služieb

Browse Private Service

+ Add Edit Delete Where Used

Filter: Filter Clear

Name	Protocol	Source Ports	Destination Po...	ICMP	Description
 sip	tcp-udp		5060		
 sunrpc	tcp-udp		111		
 tacacs	tcp-udp		49		
 talk	tcp-udp		517		
 alterna...	icmp			6	
 conver...	icmp			31	
 echo	icmp			8	
 echo-r...	icmp			0	
 inform...	icmp			16	
 inform...	icmp			15	
 mask-r...	icmp			18	
 mask-r...	icmp			17	
 mobile...	icmp			32	
 param...	icmp			12	
 redirect	icmp			5	
 router...	icmp			9	
 router...	icmp			10	
 source...	icmp			4	
 time-ex...	icmp			11	
 timest...	icmp			14	

Selected Private Service

Private Service ->

OK Cancel

DMZ – zhrnutie

Add Public Server

Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface, address of the server, and the service to be exposed. Finally, specify the public interface, address, and service in which the server will be seen.

Private Interface:

Private IP Address:

Private Service:

Public Interface:

Public IP Address:

Options

Specify Public Service if different from Private Service. This will enable the static PAT.

Public Service (TCP or UDP service only) ⓘ

OK Cancel Help

10.1 ASA Security Device Manager (ASDM)

Nové ACL

The screenshot shows the Cisco ASDM interface for configuring Firewall Access Rules. The left sidebar contains a 'Device List' and a 'Device Setup' section with options like Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management. The main area is titled 'Configuration > Firewall > Access Rules' and features a table of rules and an 'Addresses' panel on the right.

#	Enabled	Source	User
dmz (1 implicit incoming rule)			
1	<input type="checkbox"/>	any	
inside (1 implicit incoming rule)			
1	<input type="checkbox"/>	any	
outside (1 incoming rule)			
1	<input checked="" type="checkbox"/>	any4	
Global (1 implicit rule)			
1	<input type="checkbox"/>	any	

The 'Addresses' panel on the right shows a list of network objects:

- any
- any4
- any6
- dmz-network/24
- DMZ-Server
- inside-network/24
- outside-network/29
- 209.165.200.227

At the bottom, a status bar indicates 'Configuration changes saved successfully.' and the user 'admin01' is logged in. The system time is 12/3/19 7:37:05 PM.

Monitoring prevádzky v ASDM

QEMU (PC-B) - TightVNC Viewer

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > Interface Graphs > outside

Select one or more of the available graphs for the current graph type and add them to the selected graph list on the right. To display graphs for more than one graph type, select another graph type in the tree on the far left and continue adding graphs to the selected graph list.

Up to four graphs can be displayed in one window. To use an already existing graph window, select the window title from the drop-down list below. To display graphs in a new window, type in a new window title.

Graph Window Title: Cisco ASDM 7.9(2) for ASA - 192.168.1.1 - Graph (3)

Graph Selection

Available Graphs:

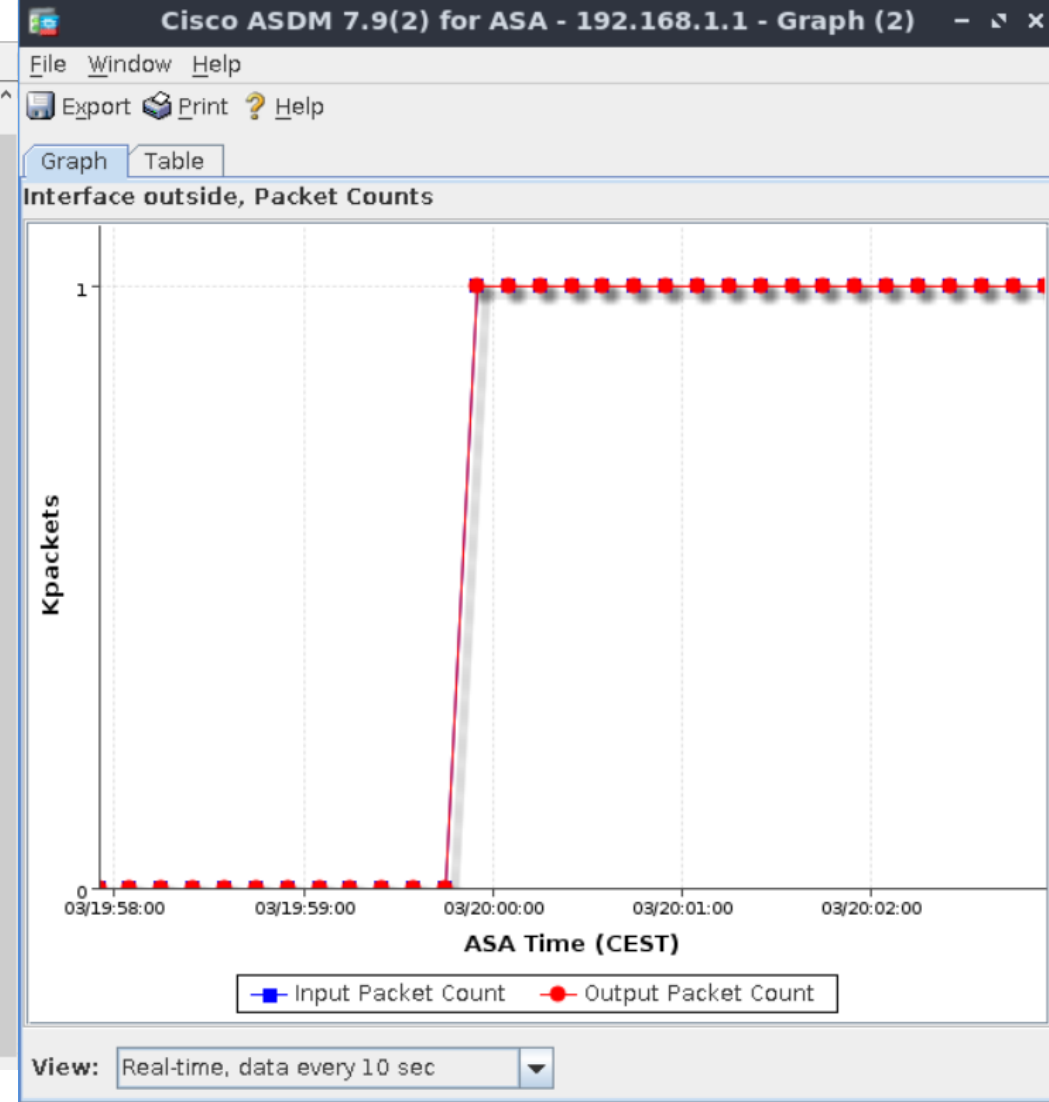
- Byte Counts
- Packet Rates
- Bit Rates
- Drop Packet Count
- Buffer Resources
- Packet Errors
- Miscellaneous
- Collision Counts
- Input Queue
- Output Queue

Selected Graphs:

- Interface outside, Packet Counts

Show Graphs...

Data Refreshed Successfully. admin01 15 12/3/19 8:01:55 PM CES





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

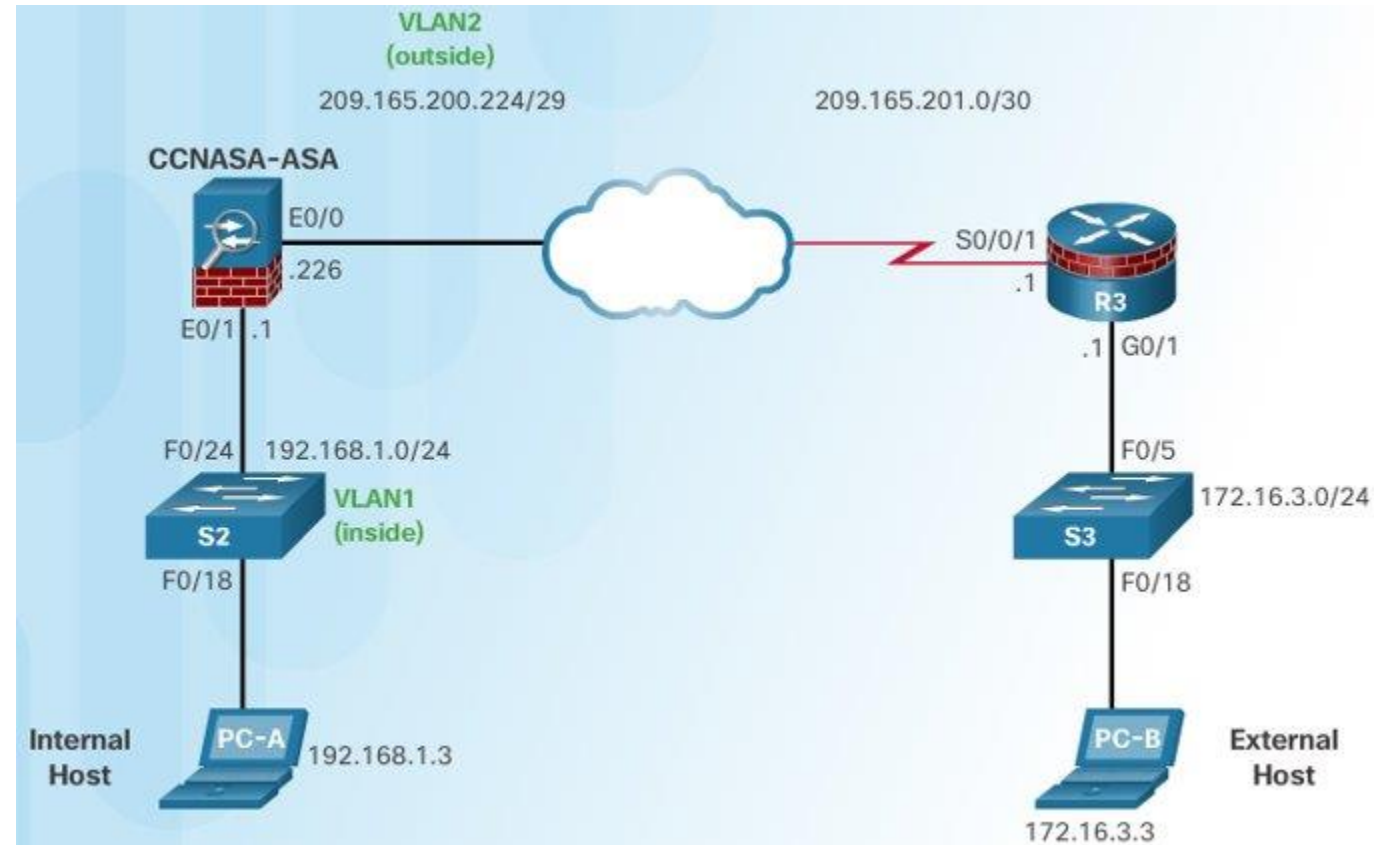
- Vytvorenie VPN spojenia medzi inou ASA alebo ISR (Integrated Service Routers)
- Komunikácia prostredníctvom vytvorením zabezpečeného pripojenia cez sieť TCP / IP (internet)
- Šifrovanie

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



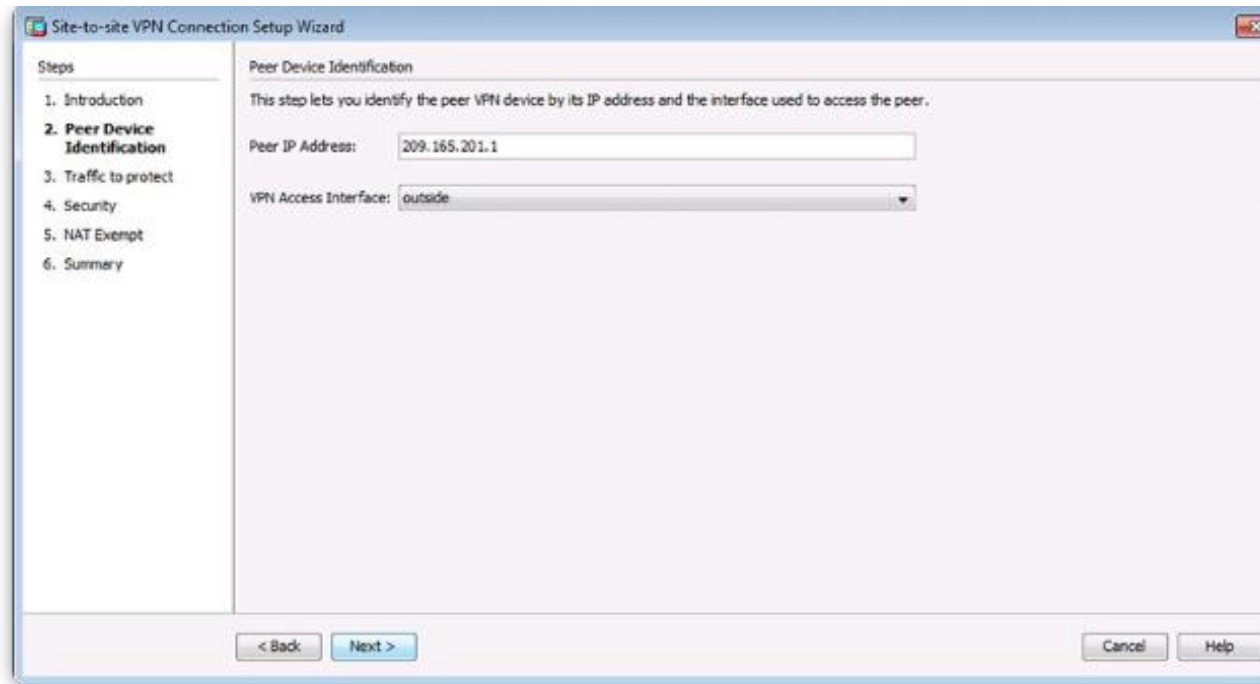
Konfigurácia ASA Site-to-site VPN použitím ASDM

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



10.2. ASA VPN Configuration

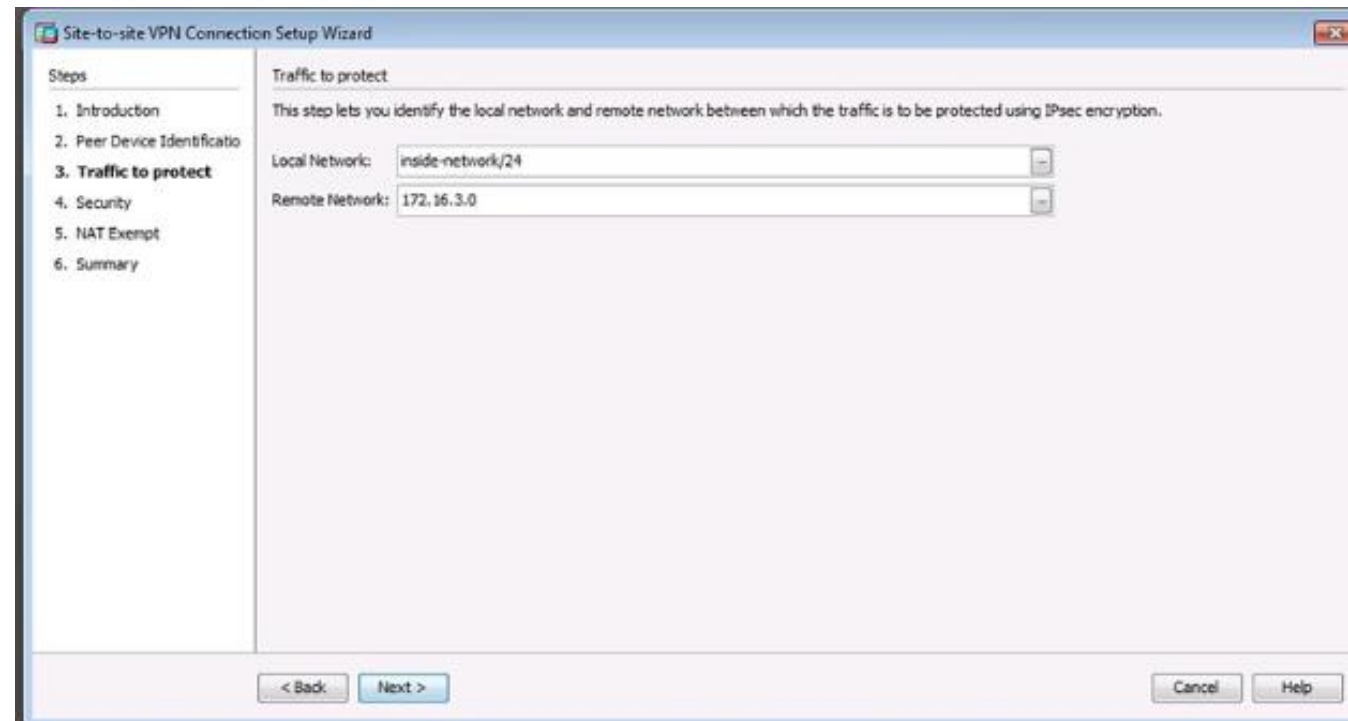
- **Step 2. Identify the peer device**



The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window. The title bar reads 'Site-to-site VPN Connection Setup Wizard'. On the left, a 'Steps' pane lists: 1. Introduction, 2. Peer Device Identification (highlighted), 3. Traffic to protect, 4. Security, 5. NAT Exempt, and 6. Summary. The main area is titled 'Peer Device Identification' and contains the text: 'This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.' Below this, there are two input fields: 'Peer IP Address:' with the value '209.165.201.1' and 'VPN Access Interface:' with a dropdown menu showing 'outside'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

10.2. ASA VPN Configuration

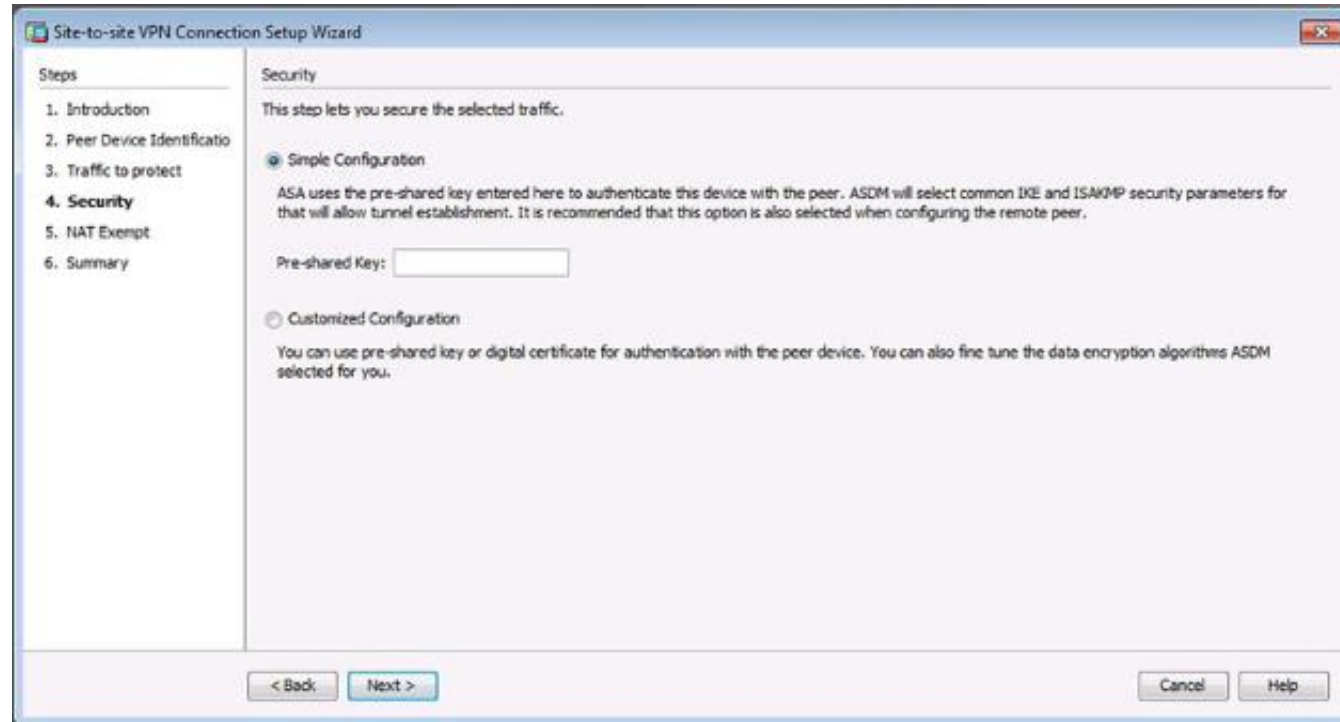
- **Step 3. Identify interesting traffic**



The screenshot shows the 'Site-to-site VPN Connection Setup Wizard' window. The title bar reads 'Site-to-site VPN Connection Setup Wizard'. On the left, a 'Steps' pane lists: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect (highlighted), 4. Security, 5. NAT Exempt, and 6. Summary. The main area is titled 'Traffic to protect' and contains the text: 'This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.' Below this text are two input fields: 'Local Network:' with the value 'inside-network/24' and 'Remote Network:' with the value '172.16.3.0'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

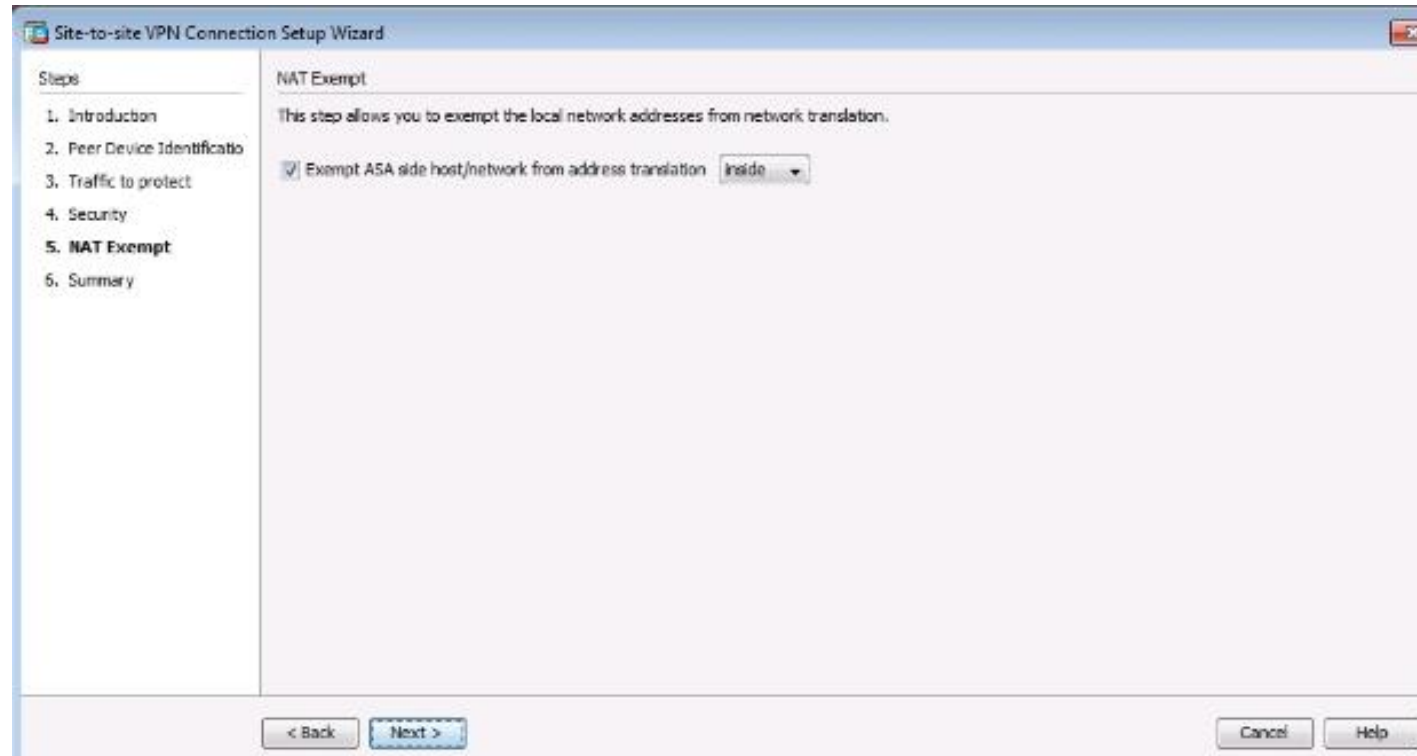
10.2. ASA VPN Configuration

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



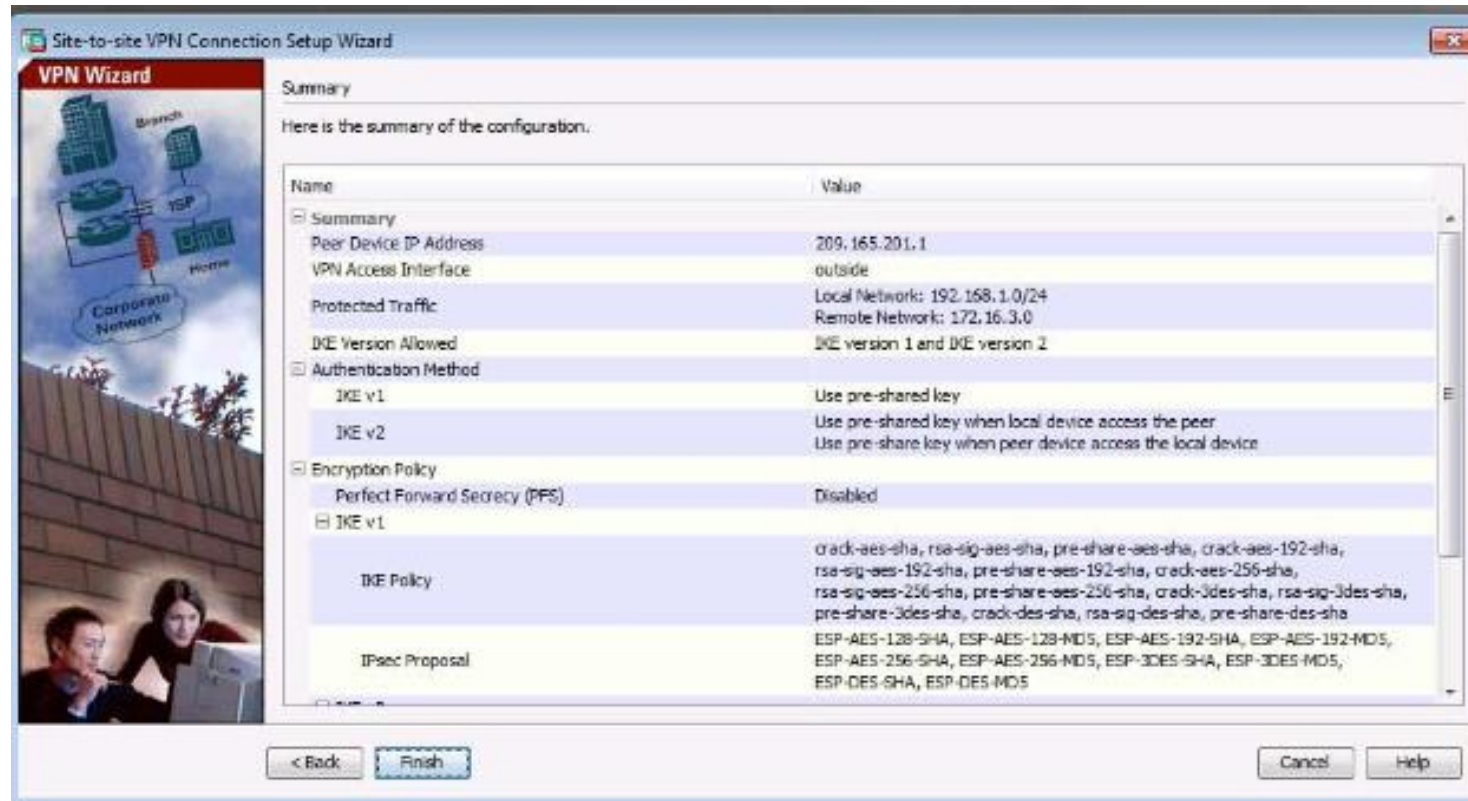
10.2. ASA VPN Configuration

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



10.2. ASA VPN Configuration

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



10.2. ASA VPN Configuration

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

The screenshot displays the Cisco ASDM 7.4 interface for an ASA device at IP 192.168.1.1. The left-hand navigation pane shows the 'VPN' section expanded to 'Sessions'. The main content area is titled 'Monitoring > VPN > VPN Statistics > Sessions'. It features a summary table and a detailed session table.

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN		1	1	1
IKEv1 IPsec		1	1	1

Filter By: [Site-to-Site] [All Sessions] [Filter]

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
0.0.0.0	IKEv1 IPsec	02:20:41 UTC Tue Apr 21 2015	100
0.0.0.0	IKEv1 (L2LDES) IPsec (10)	02:20:41 UTC Tue Apr 21 2015	100

Buttons: Details, Logout, Ping

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: [All Sessions] [Logout Sessions] [Refresh]

Last Updated: 4/21/15 3:24:15 PM

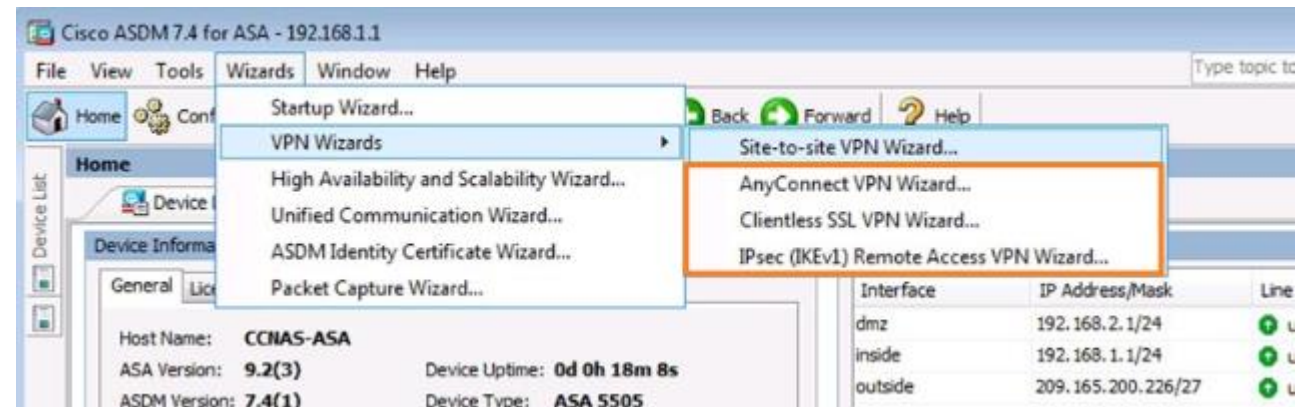
Data Refreshed Successfully. ADMIN 2 4/21/15 10:23:17 PM UTC

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

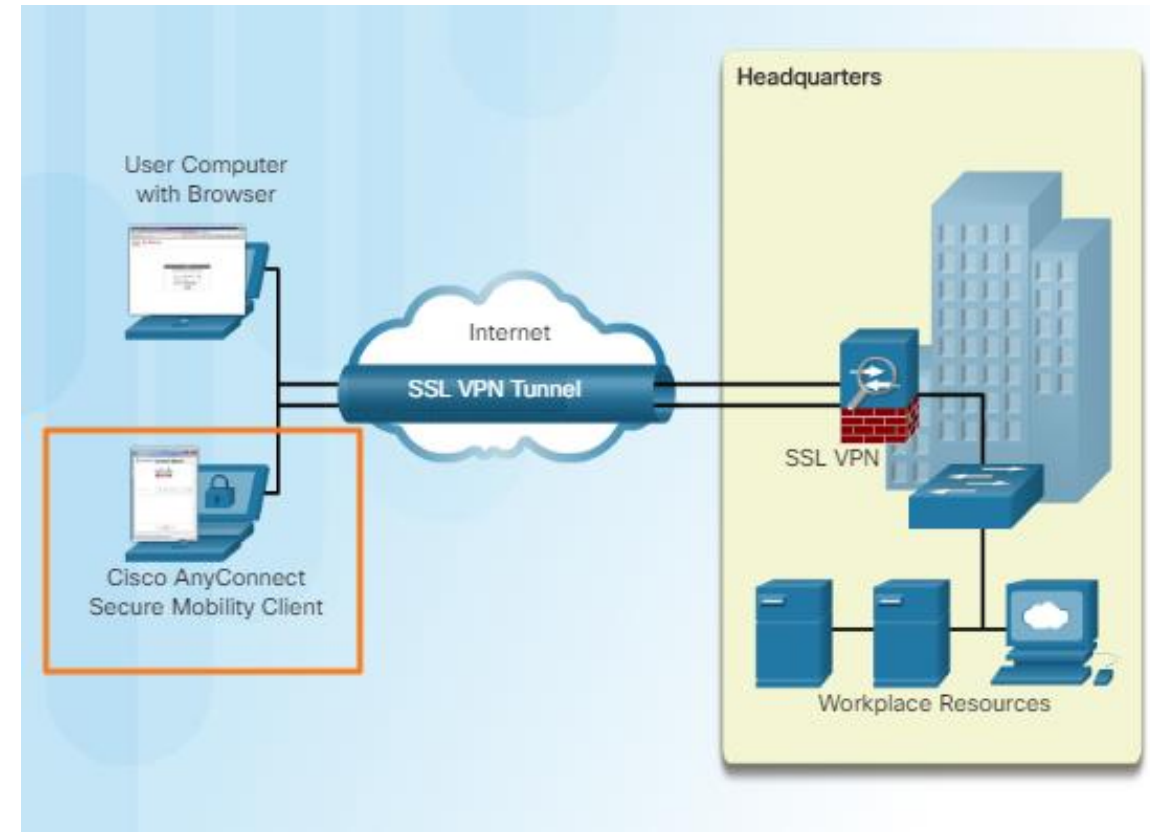
ASA SSL VPNs

- 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



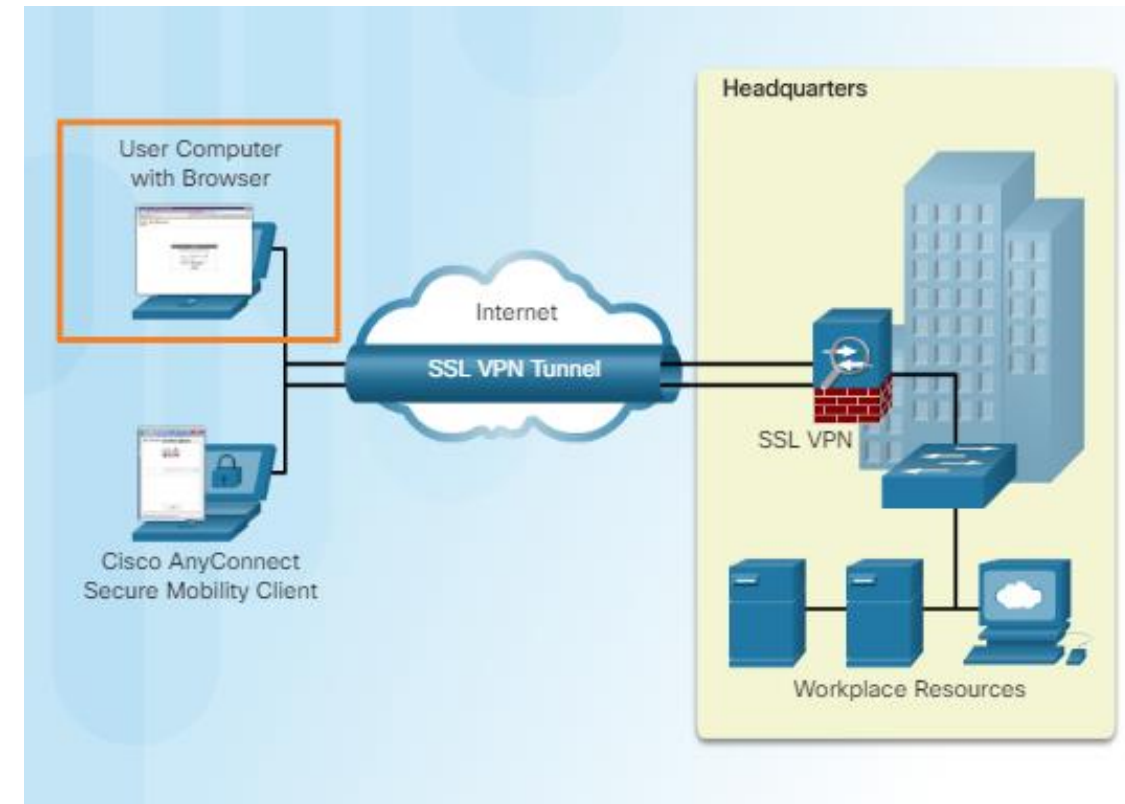
Client-Based SSL VPN

- 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



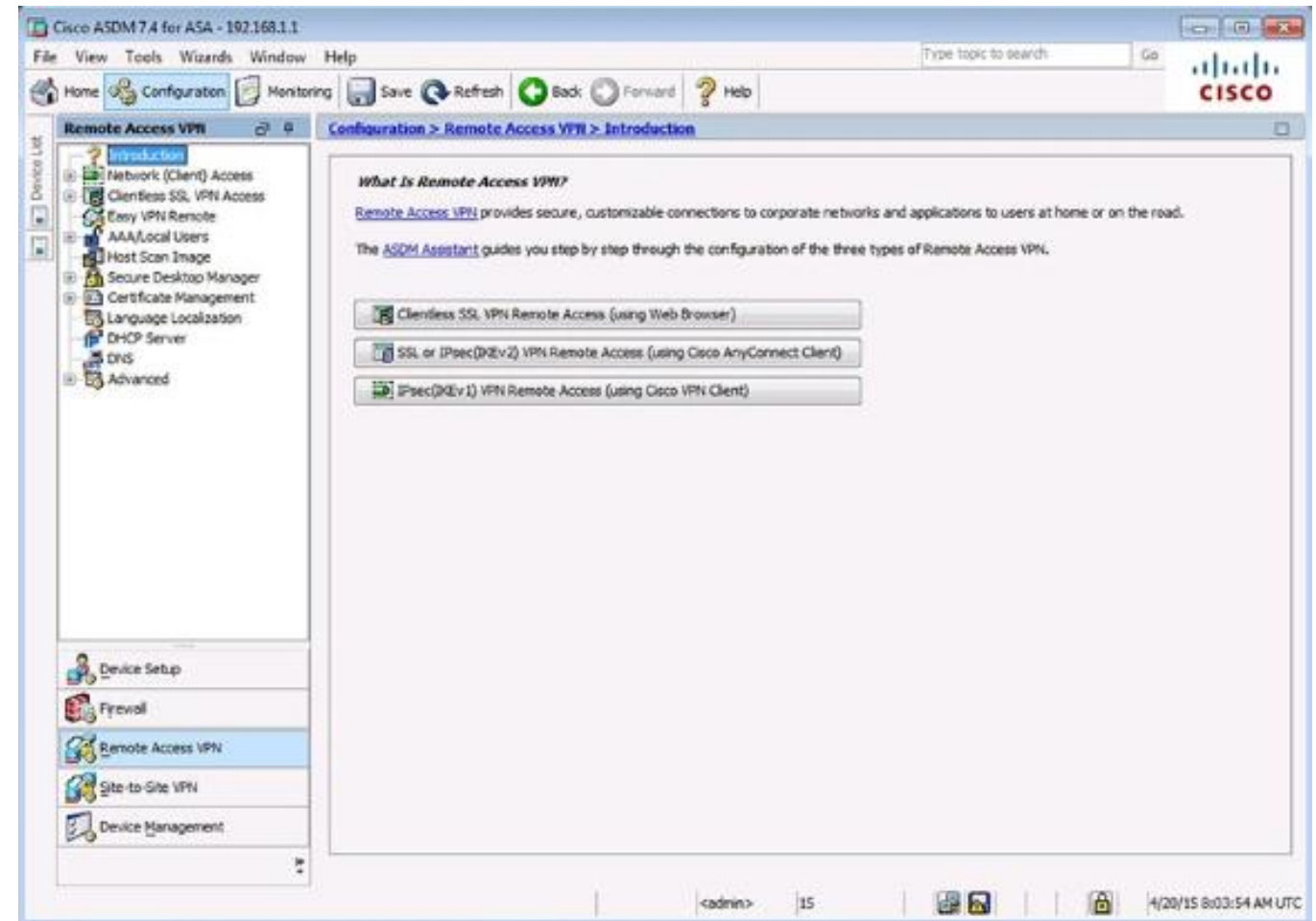
Clientless SSL VPN

- 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 sieti s využitím port-forwardingu
- Jednoduchšie na nasadenie ako client-based SSL VPN



Konfigurácia Clientless SSL VPN na ASA

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



Networking
Academy

Ďakujem za pozornosť