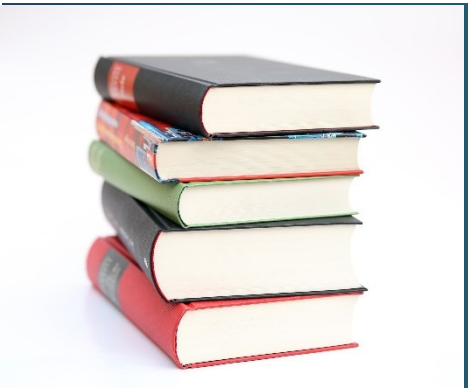
UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

# Kapitola 9: Implementácia adaptívneho bezpečnostného zariadenia (ASA) Cisco


## CCNA Security v2.0 / Network Security 1.0



Aktualizované v rámci projektu KEGA 026TUKE-4/2021.



# Osnova kapitoly

- 9.0 Úvod
- 9.1 Úvod do ASA
- 9.2 Konfigurácia firewallu ASA
- 9.3 Zhrnutie

# Úvod

- Existuje mnoho typov firewallov:
  - packet-filtering
  - stateful
  - application gateway (proxy)
  - address-translation
  - host-based
  - transparent
  - hybrid firewalls

# Úvod - Firewally Cisco

- v rámci kurzu :
  - ISR s podporou firewallu
  - Zariadenie Cisco Adaptive Security Appliance (ASA)
    - – Out of Sale
  - + ASA 5500-X
- Realita je trochu iná
- V princípe zariadenia podľa výkonu a pre
  - SMB a malé pobočky
  - Veľké pobočky a podniky
  - Campus a datacentrá (DC)
  - Service providers (SP), veľké DC

# Next Gen Firewall

- Next Gen Firewall
  - kombinuje technológiu firewallu ASA s pokročilými funkciami Sourcefire FirePOWER na detekciu hrozieb a škodlivého softvéru.
  - Up to L7 funkcionality
  - NextGen IPS, AMP, URL Filtering, Identity management

# Cisco – aktuálny stav firewall produktov - Firepower

- 1) Firepower => Firepower Threat Defense FTD
  - Konsolidácia viac bezpečostných riešení do jedného
  - Konfig cez GUI manažment only (bez CLI) – Firepower Management Center

### Firepower 1000 Series

For SMB and branch offices. Simplified Cisco Defense Orchestrator management saves you administration time so you can spend more driving your business forward.

### Firepower 2100 Series

For large branch, commercial and enterprise needs. Select the management option that suits your environment and how you work.

### Firepower 4100 Series

For large campus and data center, create logical firewalls for deployment flexibility, inspect encrypted web traffic, protect against DDoS attacks, cluster devices for performance and high availability, scalable VPNs, block network intrusions, and more.

### Firepower 9300

For service providers and high-performance data centers, this carrier-grade modular platform enables the creation of separate logical firewalls and scalable VPNs, inspects encrypted web traffic, protects against DDoS attacks, clusters devices for performance and high availability, blocks network intrusions, and more.

# Séria 5500-X

- 2) ASA5500-X with Firepower
  - ASA + Firepower Service modul + SSD disk (na ňom je Firepower virtuálka)
  - Konfig GUI or CLI, náplň kurzu
- 3) Virtuall cloud firewalls (Public/Private)

ASA 5516-X with FirePOWER Services

- Up to 900 Mbps FW
- Multiservice capable
- 8 x 1 GE
- 1 RU

ASA 5508-X with FirePOWER Services

- Up to 500 Mbps FW
- Multiservice capable
- 8 x 1 GE
- 1 RU


ASA 5506-X with FirePOWER Services

- Up to 300 Mbps FW
- Multiservice capable
- 8 x 1 GE
- Desktop

# „Životnost“ modelov X

ASA 5506-X with FirePOWER Services
Status: Available | Release Date: 17-Feb-2015

ASA 5506H-X with FirePOWER Services
Status: Available | Release Date: 30-Apr-2015

ASA 5506W-X with FirePOWER Services
Status: Available | Release Date: 07-Apr-2015

ASA 5508-X with FirePOWER Services
Status: Available | Release Date: 07-Apr-2015

ASA 5512-X with FirePOWER Services
Status: End of Sale EOL Details | End-of-Support Date: 31-Aug-2022

ASA 5515-X with FirePOWER Services
Status: End of Sale EOL Details | End-of-Support Date: 31-Aug-2022

ASA 5516-X with FirePOWER Services
Status: Available | Release Date: 07-Apr-2015

ASA 5525-X with FirePOWER Services
Status: Available | Release Date: 17-Jul-2014

ASA 5545-X with FirePOWER Services
Status: Available | Release Date: 17-Jul-2014

ASA 5555-X with FirePOWER Services
Status: Available | Release Date: 17-Jul-2014

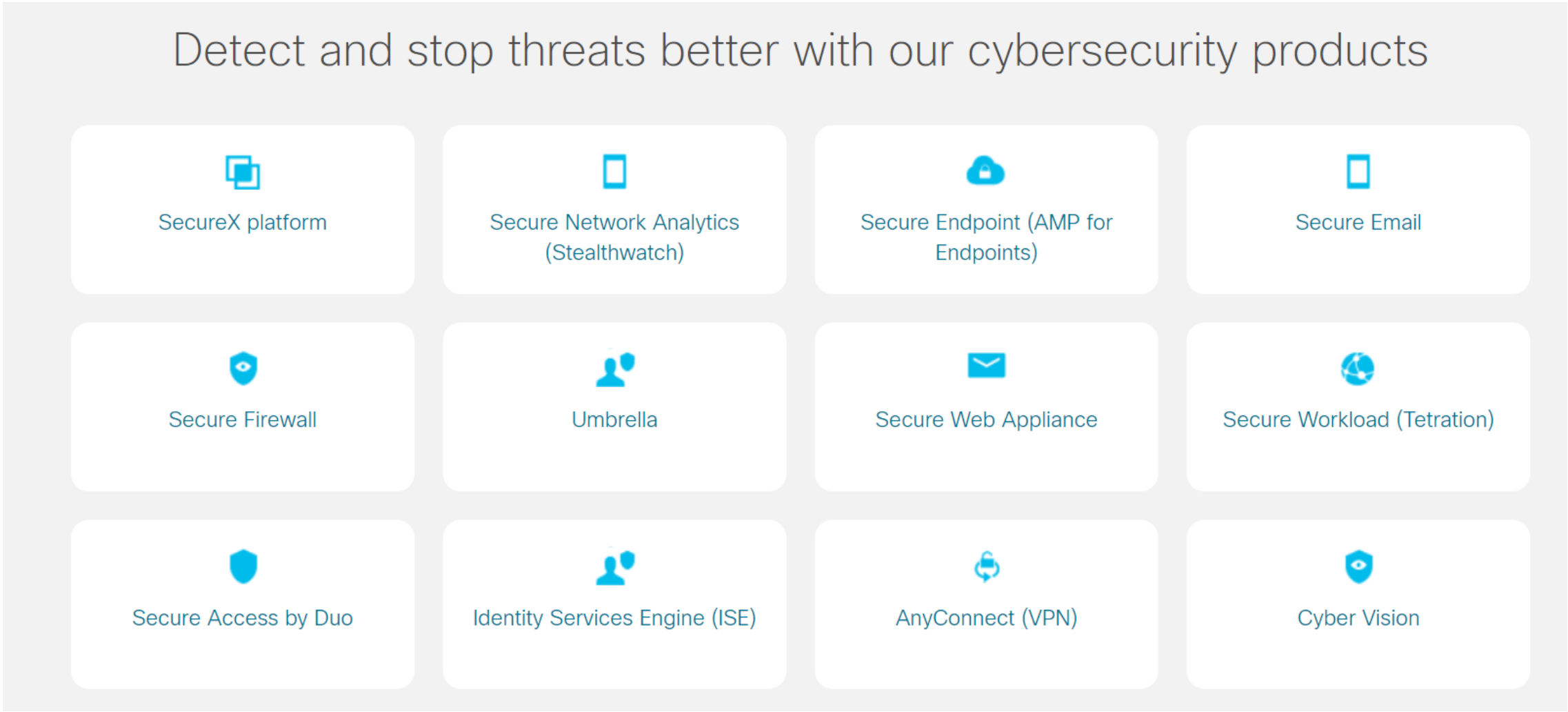
ASA 5585-X with FirePOWER SSP-10
Status: End of Sale EOL Details | End-of-Support Date: 31-Aug-2022

ASA 5585-X with FirePOWER SSP-20
Status: End of Sale EOL Details | End-of-Support Date: 31-Aug-2022

ASA 5585-X with FirePOWER SSP-40
Status: End of Sale EOL Details | End-of-Support Date: 31-Aug-2022

ASA 5585-X with FirePOWER SSP-60
Status: End of Sale EOL Details | End-of-Support Date: 31-Aug-2022

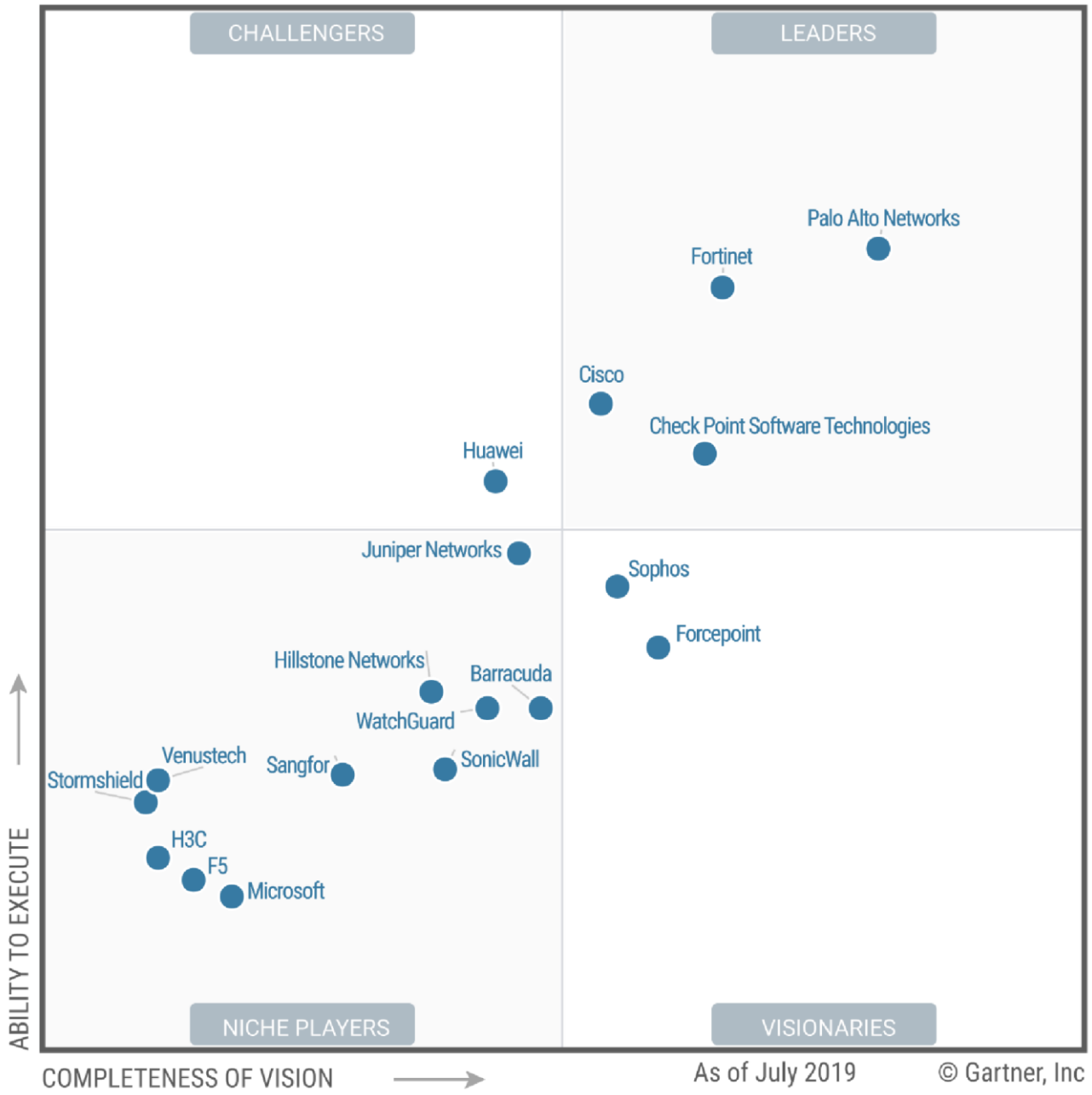
# Bezpečnosť vo vrstvách - Cisco



# Gartner Magic Quadrant report

- Situácia na trhu, platený report
  - tu enterprise firewalls 2020

Figure 1. Magic Quadrant for Network Firewalls



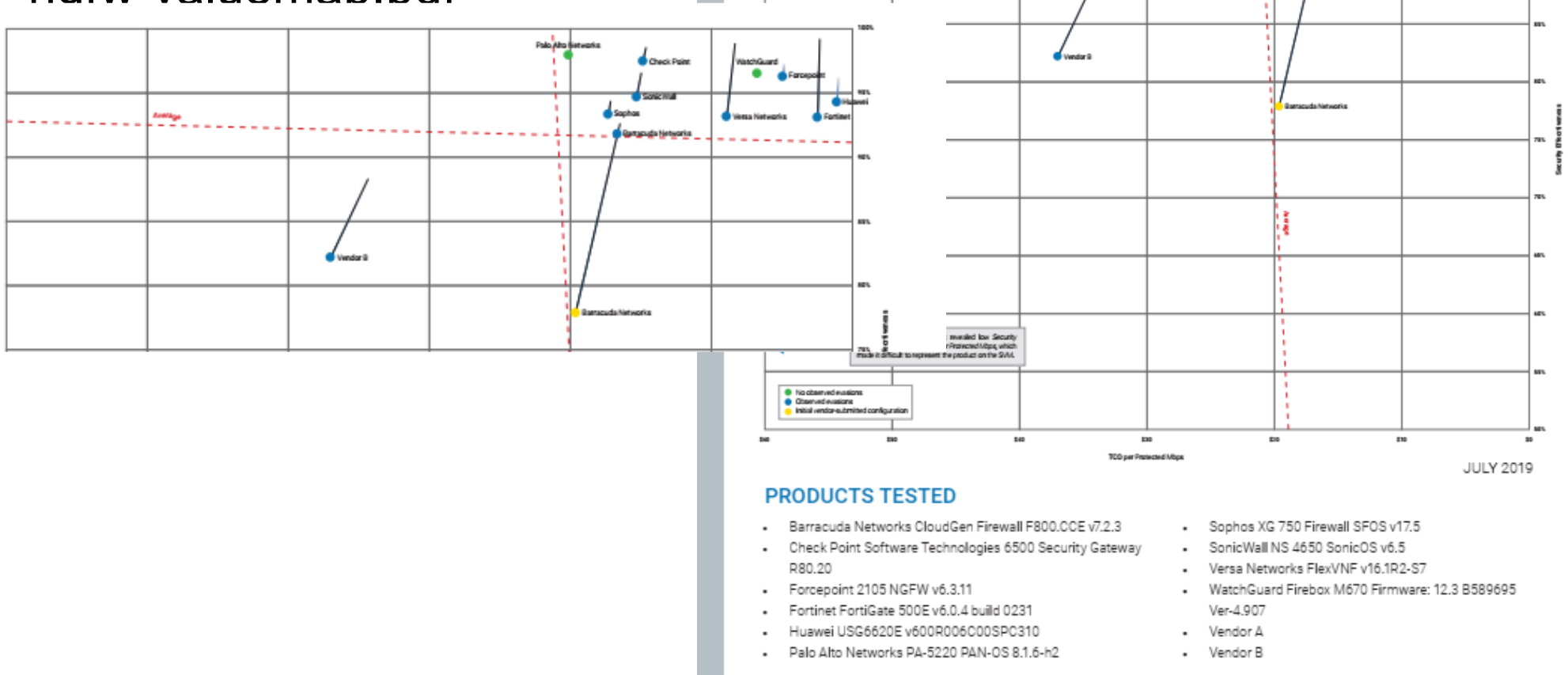

Source: Gartner (September 2019)

# NSS Labs

- Situácia na trhu, voľný prístup
  - tu NextGen firewalls 2019

| Vendor | Block Rate | Evasions | Stability and Reliability | Security Effectiveness |
|---|---|---|---|---|
| Barracuda Networks | 92.7% | 99% | 100% | 91.7% |
| Check Point Software Technologies | 98.4% | 99% | 100% | 97.4% |
| Forcepoint | 97.2% | 99% | 100% | 96.2% |
| Fortinet | 99.0% | 94% | 100% | 93.0% |
| Huawei | 96.2% | 98% | 100% | 94.2% |
| Palo Alto Networks | 97.9% | 100% | 100% | 97.9% |
| SonicWall | 97.6% | 97% | 100% | 94.7% |
| Sophos | 94.2% | 99% | 100% | 93.3% |
| Versa Networks | 99.0% | 94% | 100% | 93.1% |
| WatchGuard | 96.5% | 100% | 100% | 96.5% |
| Vendor A | 98.3% | 79% | 100% | 77.7% |
| Vendor B | 88.4% | 93% | 100% | 82.2% |

- https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2019-ngfw-valuemap.pdf



# 9.1 Úvod do ASA

**Po dokončení tejto časti by ste mali byť schopní:**

Porovnať riešenia ASA s inými firewall smerovacími technológiami .

Vysvetliť ASA 5505 s predvolenou konfiguráciou.

# IOS Firewall vs ASA firewall – Prečo ASA?

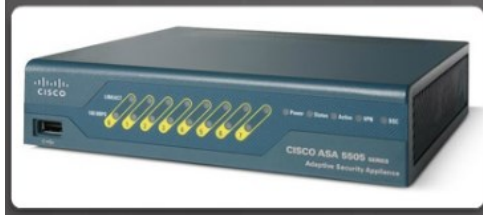
- IOS Firewall
  - Pre malé podniky
  - Pre adminov oboznámených s IOS OS
  - Problém s výkonom a škálovateľnosťou pre väčšie firmy
- Riešenie => ASA firewall
  - Adaptive Security Appliance
  - Alebo lepšie dnes
    - NextGen Firewall = ASA FW + FirePower upper layer inspection (kúpené 2013)

- ASA-X
  - Pôvodná ASA 5500:
    - End of Sale, End of Live
    - Stále veľmi rozšírená, Bez NextGen funkcií
  - X rada poskytuje
    - Overená technológia stavového FW
      - Extra config features
    - Výkonné riešenie VPN
      - L3 – IPSec, bez obmedzenia
      - L4 SSL, default 2 licencie
    - Failover redundancia
      - Licencované
    - Škálovateľosť výkonu
      - Modelové rady
      - + podporné moduly
    - NextGen Features
      - IPS (cez FirePOWER službu)
      - Advanced Malware Protection (AMP)
      - Application control/visibility (SSL inspection), URL filtering
      - Identity

Malé podniky

# ASA firewall modely

- Aktuálny stav?
  - S Firepower 5506-X/5508-X/5516-X
  - Iné, ak sú, tak ako klasické ASA



| | |
|---|---|
| ASA 5505 / Security Plus | Up to 150 Mbps |

| | |
|---|---|
| ASA 5506-X/Security Plus | 750 Mbps |

| | |
|---|---|
| ASA 5512-X/Security Plus | 1 Gbps |
| ASA 5515-X | 1.2 Gbps |

Stredné a veľké podniky

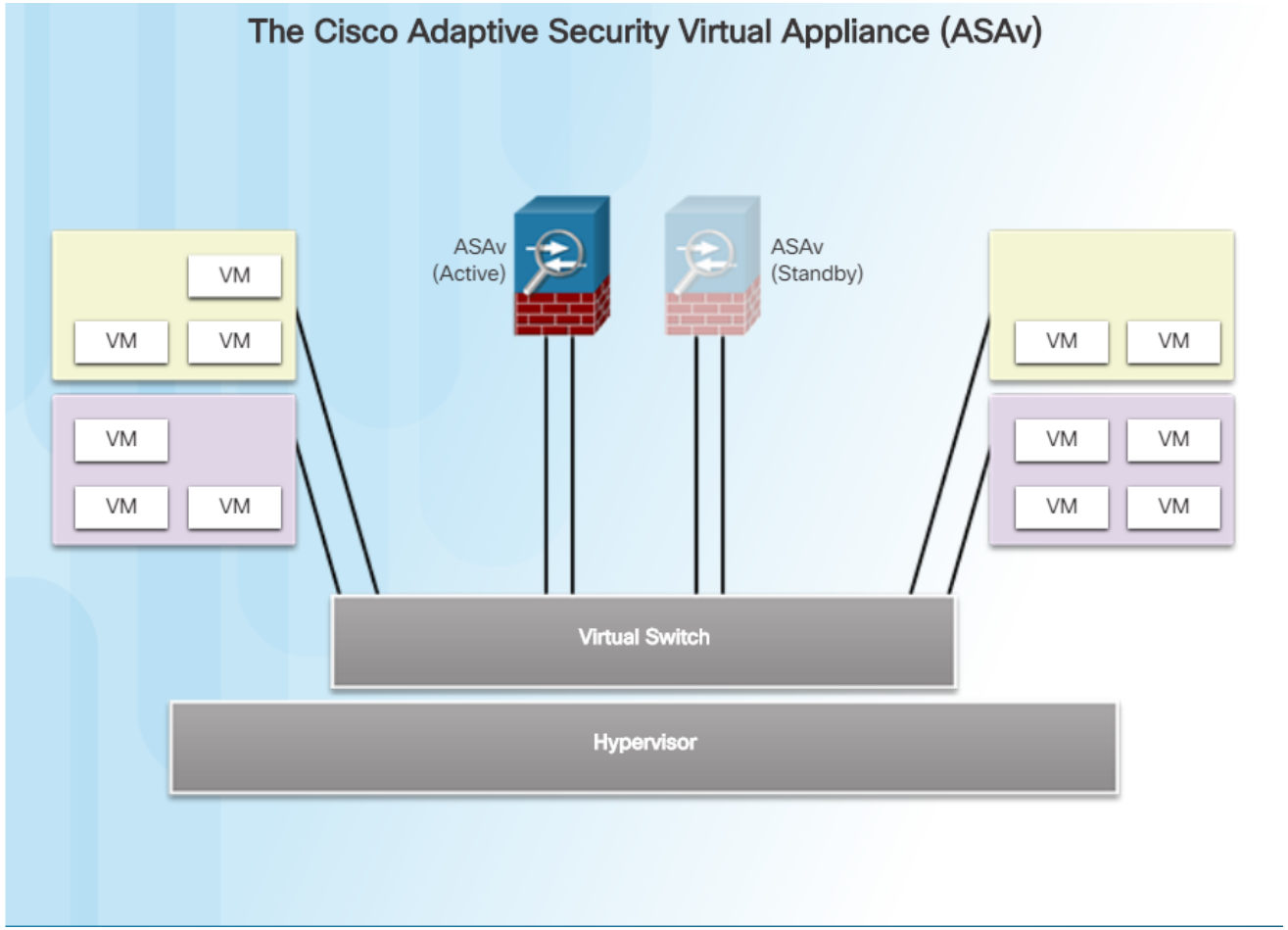
| | |
|---|---|
| ASA 5525-X | 2 Gbps |
| ASA 5545-X | 3 Gbps |
| ASA 5555-X | 4 Gbps |

| | |
|---|---|
| ASA 5585-X SSP10 | 4 Gbps |
| ASA 5585-X SSP20 | 10 Gbps |
| ASA 5585-X SSP40 | 20 Gbps |
| ASA 5585-X SSP60 | 40 Gbps |

**Veľké podniky a data centrá**

| | |
|---|---|
| ASA Service Module | 20 Gbps |

# Virtuálna ASA (ASAv)

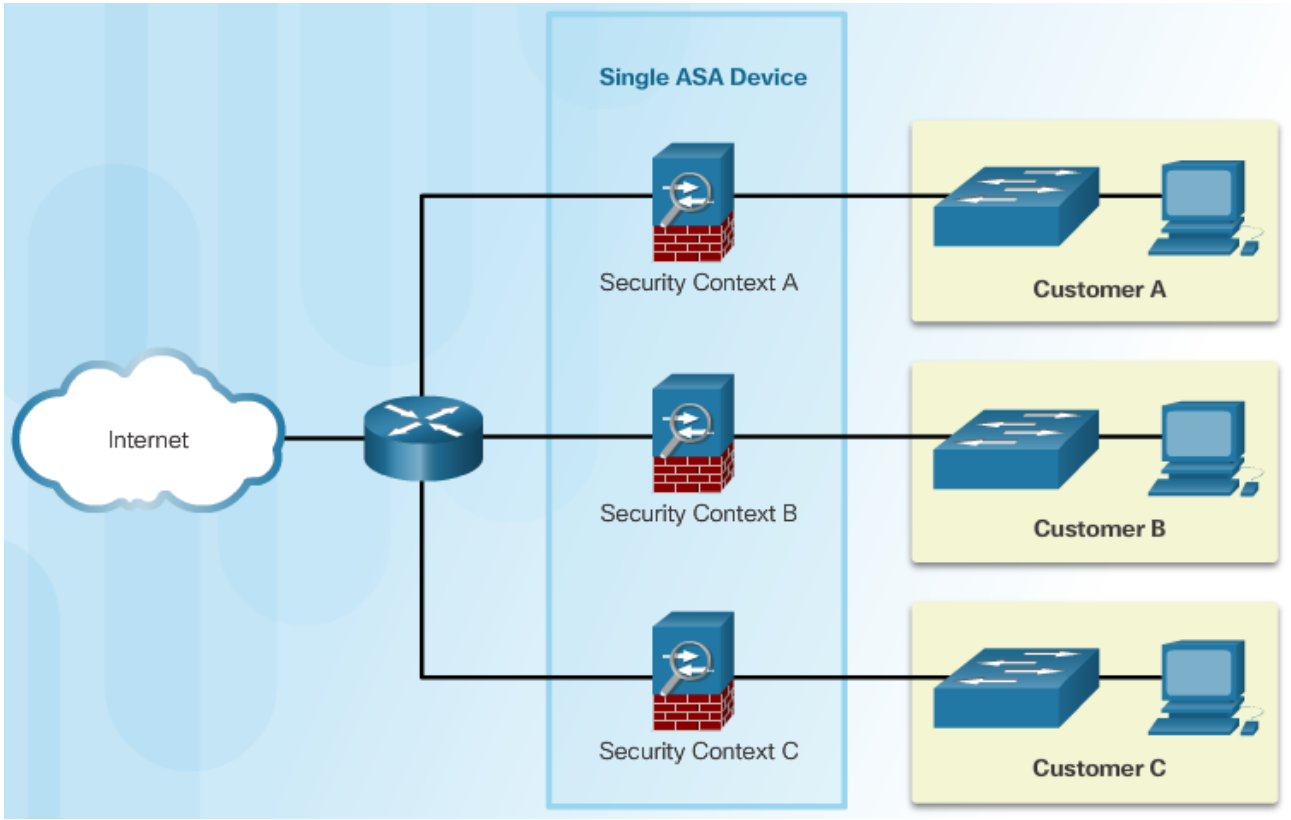



- ASAv podporuje
  - Site-to-site VPN
  - VPN so vzdialeným prístupom
  - Clientless VPN.
- ASAv je k dispozícii 4 modeloch
  - Náročnosť na RAM a priepustnosť
  - Cisco ASAv5
  - Cisco ASAv10
  - Cisco ASAv30
  - Cisco ASAv50

| Feature | ASAv5 | ASAv10 | ASAv30 | ASAv50 |
|---|---|---|---|---|
| Stateful inspection throughput (maximum)[1] | 100 Mbps | 1 Gbps | 2 Gbps | 10 Gbps |
| Stateful inspection throughput (multiprotocol)[2] | 50 Mbps | 500 Mbps | 1 Gbps | 5 Gbps |
| Advanced Encryption Standard (AES) VPN throughput[3] | 30 Mbps | 125 Mbps | 1 Gbps | 3 Gbps |
| Connections per second | 8,000 | 20,000 | 60,000 | 120,000 |
| Concurrent sessions | 50,000 | 100,000 | 500,000 | 2,000,000 |
| VLANs | 25 | 50 | 200 | 1024 |
| Bridge groups | 12 | 25 | 100 | 250 |
| IPsec VPN peers | 50 | 250 | 750 | 10,000 |
| Cisco AnyConnect® or clientless VPN user sessions | 50 | 250 | 750 | 10,000 |
| Cisco Unified Communications phone proxy | 50 | 250 | 1000 | Not tested |
| Cisco Cloud Web Security users | 250 | 1,000 | 5000 | Not tested |
| High availability | Active/standby | | | |
| Hypervisor support | VMware ESX/ESXi 6.0, 6.5; vMotion<br>KVM<br>Hyper-V: Windows Server 2012 R2 (Not supported for ASAv50) | | | |
| Public Cloud Support | AWS (c3.large, c3.xlarge, c4.large, c4.xlarge, M4)<br>Azure (d3, d3_v2) (including Azure Government Cloud) | | | Currently not supported on Public Cloud |
| Modes | Routed and transparent | | | |
| Virtual CPUs | 1 | 1 | 4 | 8 |
| Memory | 1 GB minimum<br>1.5 GB maximum | 2 GB | 8 GB | 16 GB |
| Minimum disk storage[4] | 8 GB | 8 GB | 16 GB | 16 GB |

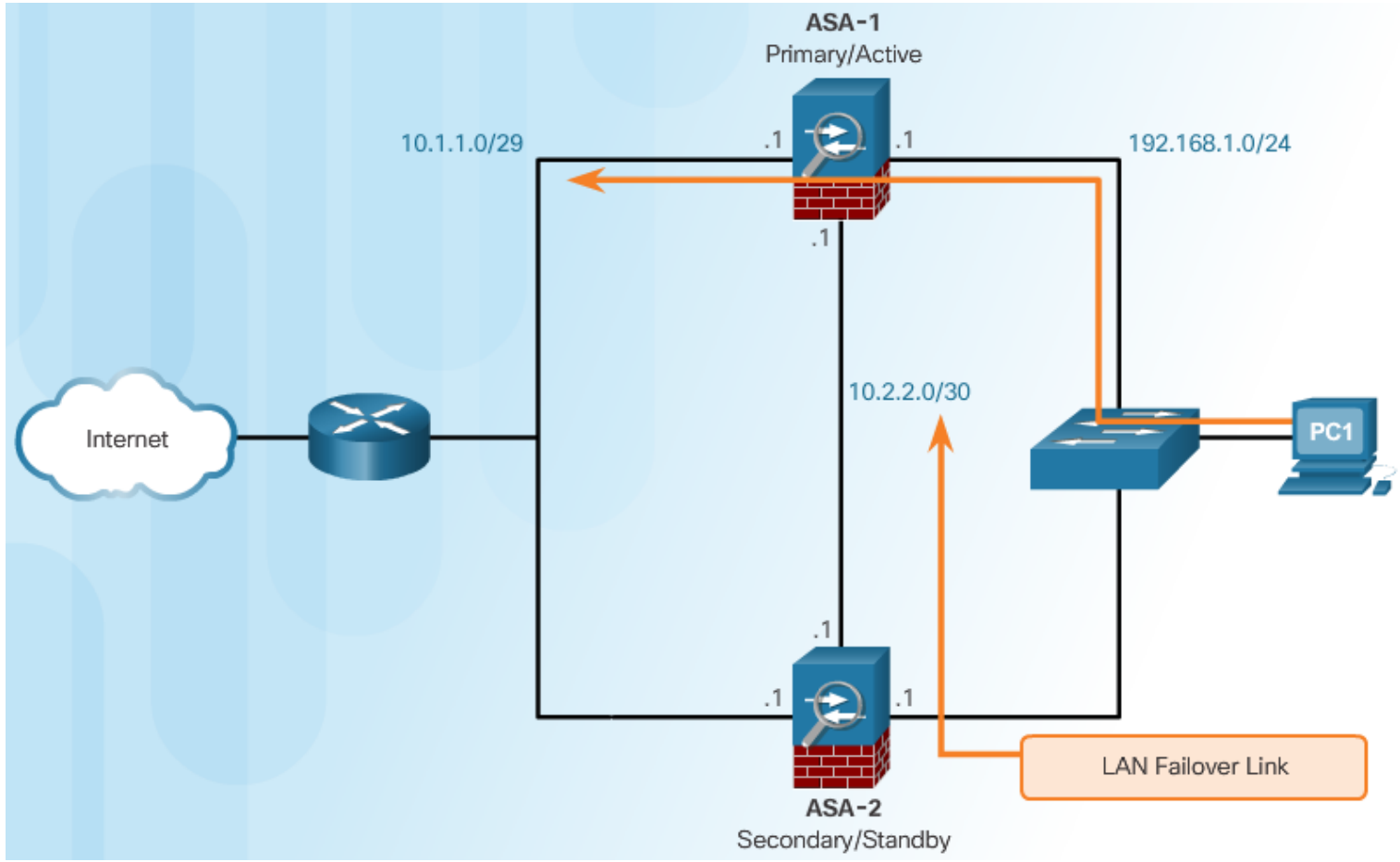
# Pokročilé vlastnosti ASA - Virtualizácia

- Jedna ASA sa môže rozdeliť na viacero virtuálnych zariadení
- Každé virtuálne zariadenie
  - sa nazýva **bezpečnostný kontext**.
  - je nezávislé zariadenie s vlastnou bezpečnostnou politikou, rozhraniami a správcami.
  - Vlastná smerovacia tabuľka, funkcie firewallu, IPS a manažment
  - **Mínus**
    - nie je podporované VPN a dynamické smerovacie protokoly.



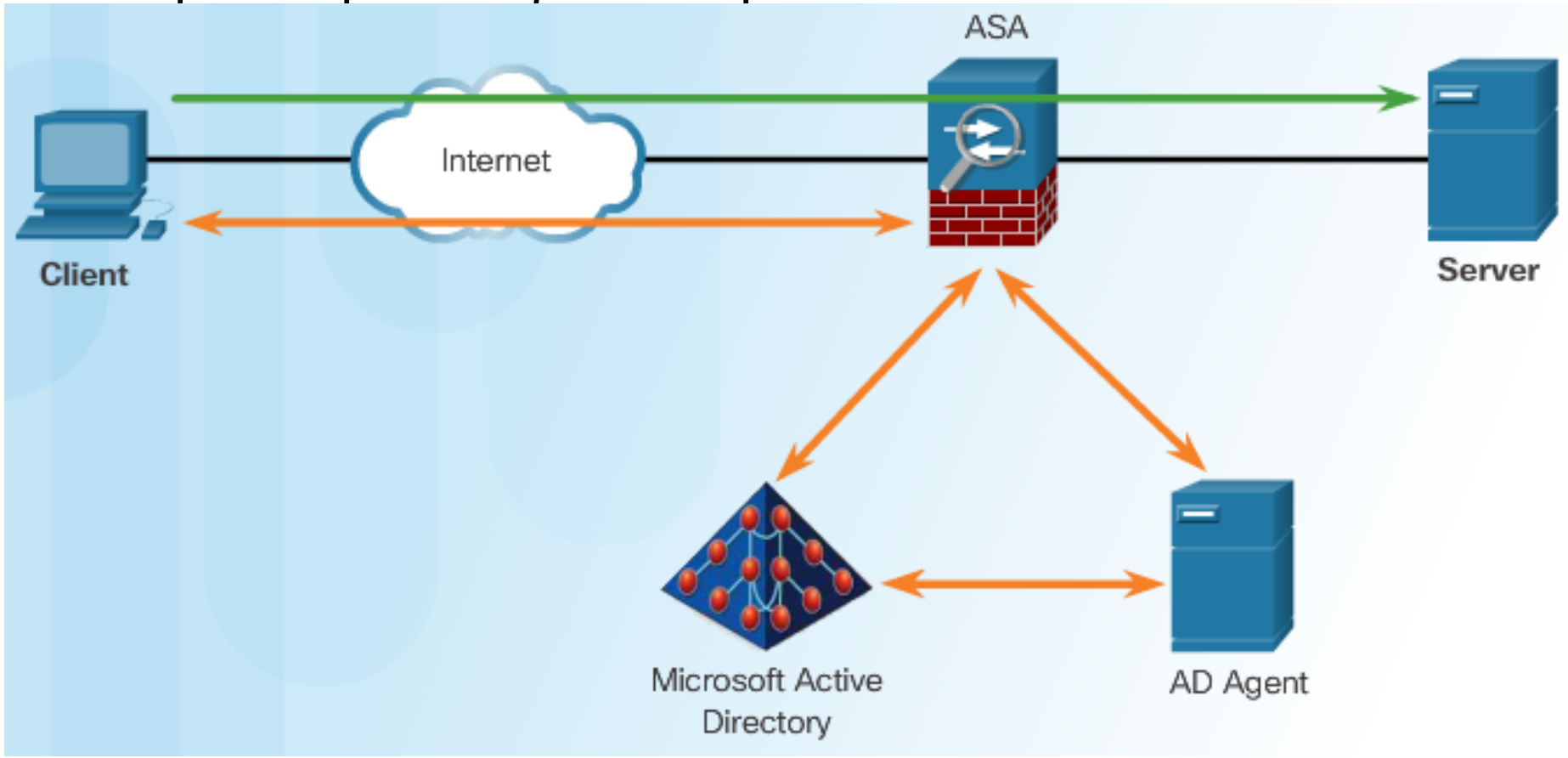
# Pokročilé vlastnosti ASA - Vysoká dostupnosť

- Tzv. Failover
  - Dve identické ASA sa môžu sparovať aby sa zabezpečila redundancia zariadenia
  - Mode Active/Standby
- Vyžaduje dedikovaný failover port
- Musia mať rovnaké
  - Identické v softvéri
  - Licencie
  - Pamäte
  - Rozhrania
  - V rátane rozširujúcich modulom bezpečnostných služieb (SSM)



# Pokročilé vlastnosti ASA - Firewall politiky s identitami

- Riadenie prístupu založené na priradení IP adries k prihlasovacím informáciám pomocou Windows Active Directory
- V ACL sa potom používajú mená používateľov

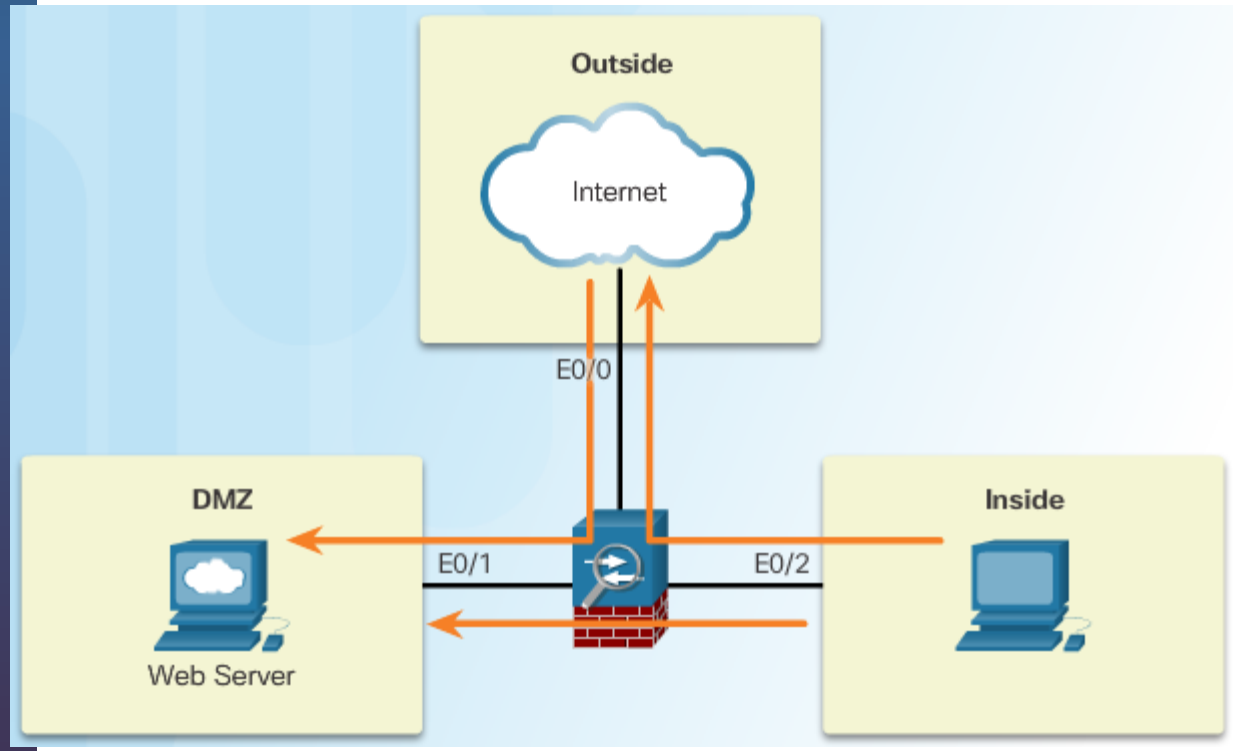


# Pokročilé vlastnosti ASA - Kontrola hrozieb (Threat control)

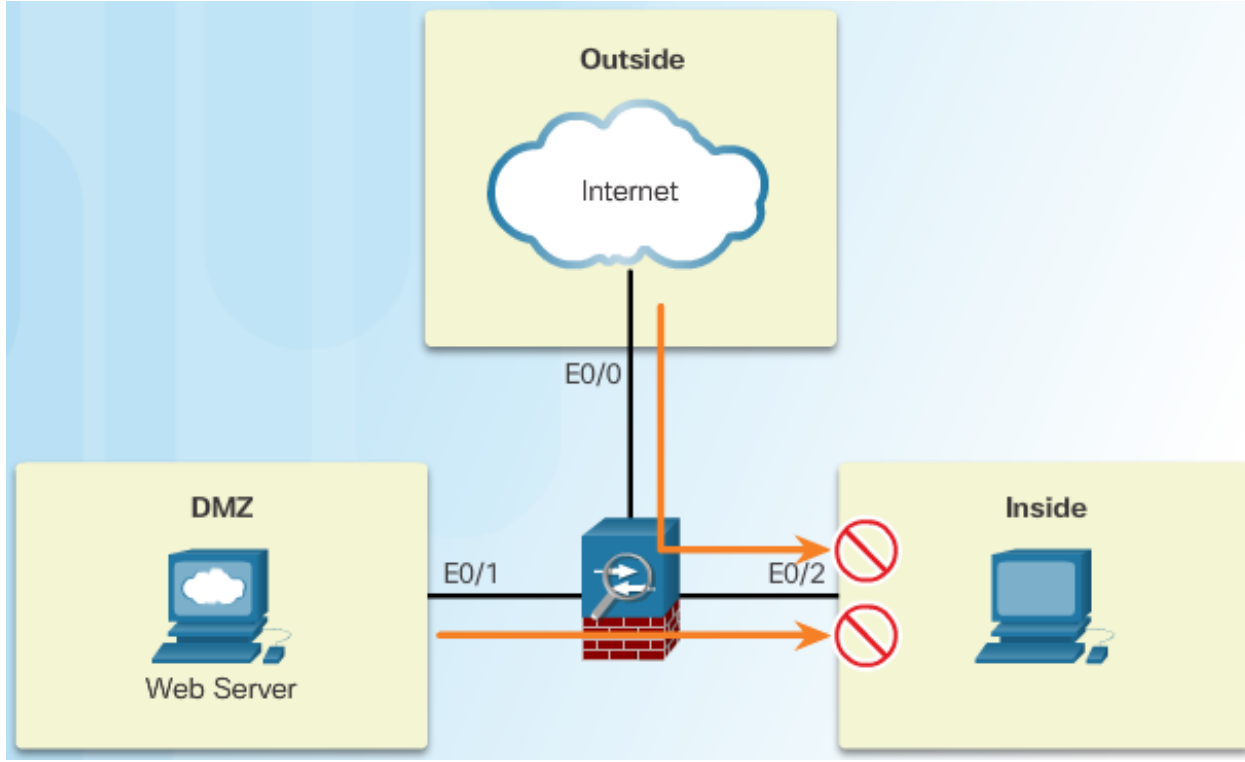
- Všetky ASA podporujú
  - Vstavané základné funkcie IPS
  - Pokročilé funkcie => K dispozícii pomocou zásuvných modulov (=> špeciálne hardvérové moduly do ASA)
    - Pokročilé IPS: Advanced Inspection and Prevention Module (AIP SSM) a card (AIP SSC)
    - Antimalwarové funkcie => modul Content Security and Control (CSC)
    - AIP-SSM a AIP-SSC poskytujú ochranu pred desiatkami tisíc známych zneužití.
      - Vhodnné aktualizovať
      - Cisco Services for IPS poskytuje aktualizácie signatúr prostredníctvom globálneho spravodajského tímu, ktorý pracuje 24 hodín denne, aby pomohol zabezpečiť ochranu pred najnovšími hrozbami.

# Pripomeňme si – úloha zónových stavových FW

- Nasadenie perimeter
- Zóny: Outside, Inside, DMZ
- Stavový FW: riadenie prístupu na zónach + ACL



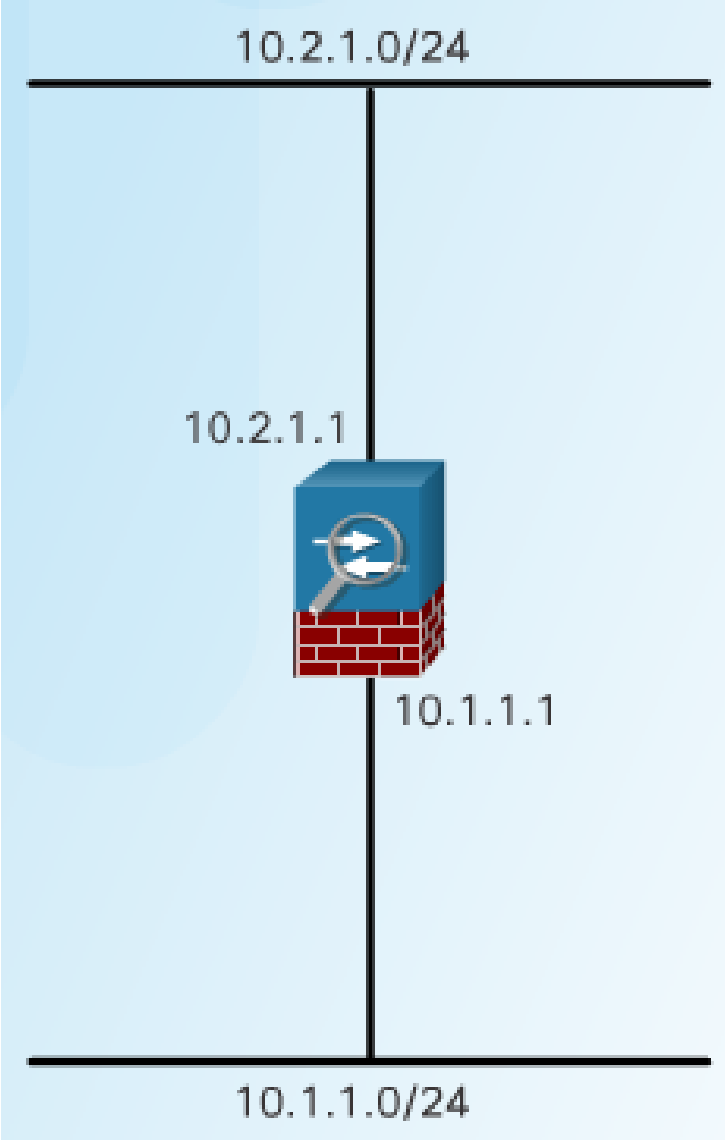

→ Povolená prevádzka




Zamietnutá prevádzka→

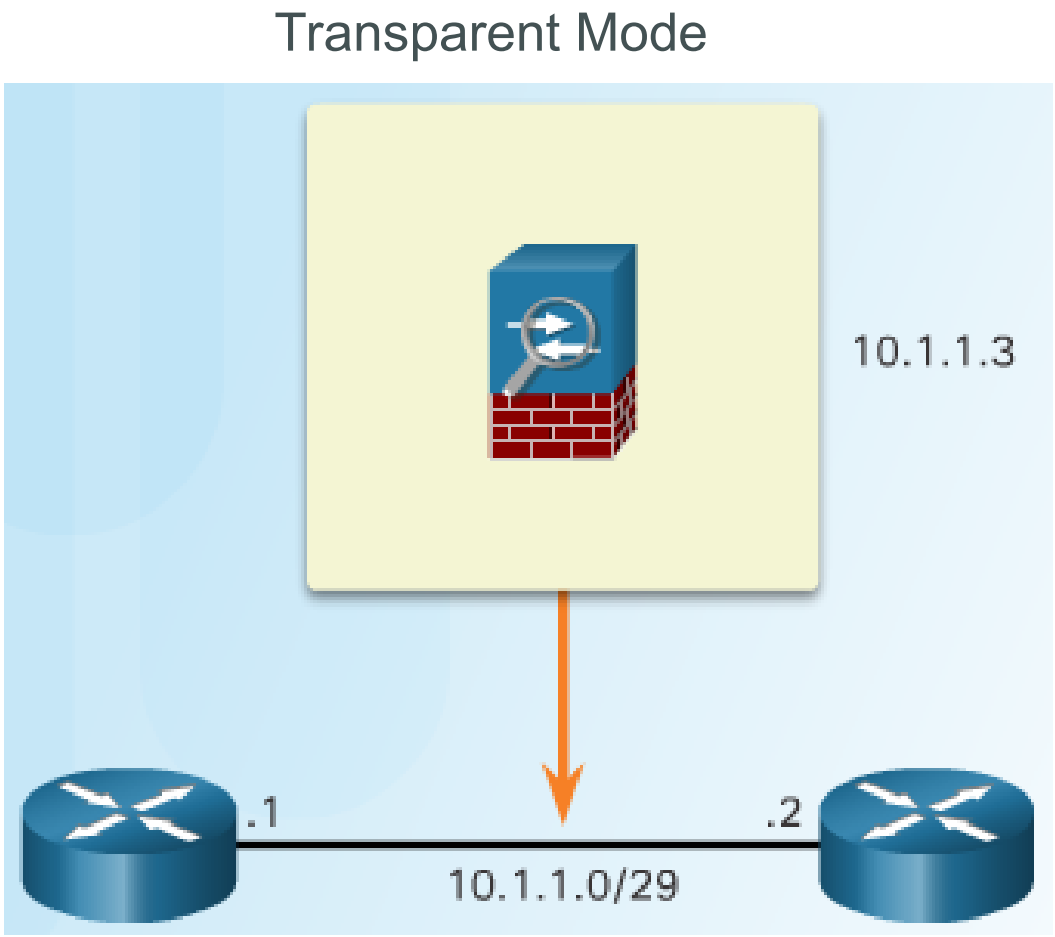
# Prevádzkové režimy ASA - Routed Mode

- L3 box s podporou smerovania
  - Dve alebo viac rozhraní oddeľujú siete L3, t. j. domény
  - Môže vykonávať NAT medzi pripojenými sieťami
  - ASA uplatňuje politiku na toky, keď prechádzajú bránou firewall



# Prevádzkové režimy ASA - Transparentný režim

- L2 režim
  - Často sa označuje ako „bump in the wire," alebo „stealth firewall".
  - Žiadne smerovanie a obmedzené L3 funkcie
    - Tento režim neobsahuje podporu pre dynamické smerovacie protokoly, VPN, QoS alebo DHCP Relay.
  - Vhodnosť
    - zjednodušenie konfigurácie siete či nasadenia
    - keď nie je možné zmeniť existujúce IP adresy.



# Licenčné požiadavky ASA

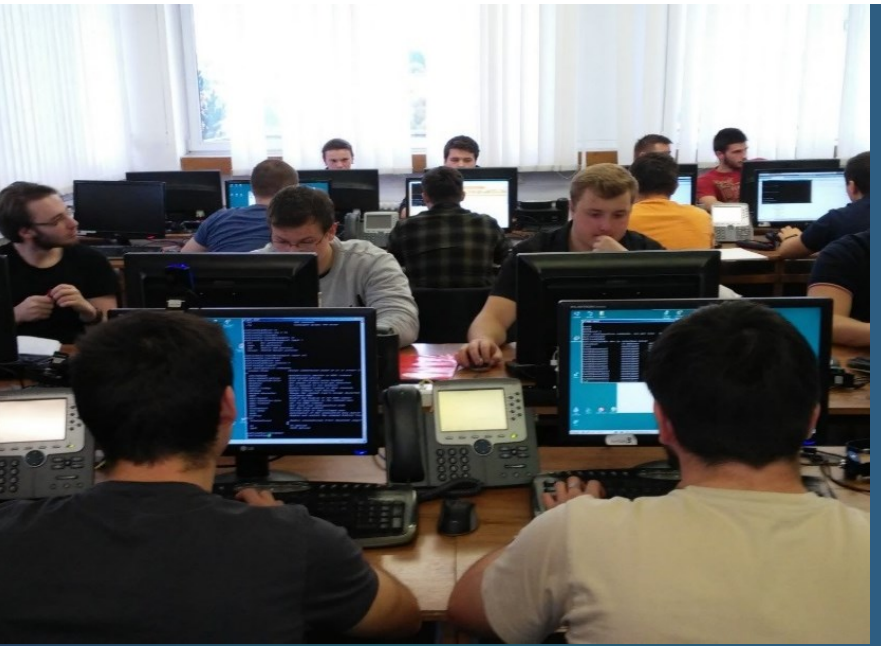
| Licenses | Description (Base License in Plaintext) | | | |
|---|---|---|---|---|
| **Firewall Licenses** | | | | |
| Botnet Traffic Filter | Disabled | *Optional Time-based license: Available* | | |
| Firewall Conns, Concurrent | 10,000 | | | |
| GTP/GPRS | No support | | | |
| Intercompany Media Engine | Disabled | *Optional license: Available* | | |
| Unified Comm. Sessions | 2 | *Optional license: 24* | | |
| **VPN Licenses** | | | | |
| Adv. Endpoint Assessment | Disabled | *Optional license: Available* | | |
| AnyConnect Essentials | Disabled | *Optional license: Available (25 sessions)* | | |
| AnyConnect Mobile | Disabled | *Optional license: Available* | | |
| AnyConnect Premium (sessions) | 2 | *Optional Permanent or Time-based licenses:* | 10 | 25 |
| Combined VPN sessions of all types, Maximum | 25 | | | |
| Other VPN (sessions) | 10 | | | |
| VPN Load Balancing | No Support | | | |
| **VPN Licenses** | | | | |
| Encryption | Base (DES) | *Opt. lic Strong (3DES/AES)* | | |
| Failover | Active/Standby (no stateful failover) | | | |
| Interfaces of all types, Max. | 120 | | | |
| Security Contexts | No Support | | | |
| Users, concurrent | 10 | *Optional licenses:* | 50 | Unlimited |
| VLANs/Zones, Maximum | Routed mode: 20<br><br>Transparent mode: 3 (2 regular zones and 1 failover link) | | | |
| VLAN Trunk, Maximum | 8 trunks | | | |

| Licenses | Description (Security Plus Lic. in Plaintext) | | | |
|---|---|---|---|---|
| **Firewall Licenses** | | | | |
| Botnet Traffic Filter | Disabled | *Optional Time-based license: Available* | | |
| Firewall Conns, Concurrent | 25,000 | | | |
| GTP/GPRS | No support | | | |
| Intercompany Media Engine | Disabled | *Optional license: Available* | | |
| Unified Comm. Sessions | 2 | *Optional license: 24* | | |
| **VPN Licenses** | | | | |
| Adv. Endpoint Assessment | Disabled | *Optional license: Available* | | |
| AnyConnect Essentials | Disabled | *Optional license: Available (25 sessions)* | | |
| AnyConnect Mobile | Disabled | *Optional license: Available* | | |
| AnyConnect Premium (sessions) | 2 | *Optional Permanent or Time-based licenses:* | 10 | 25 |
| Combined VPN sessions of all types, Maximum | 25 | | | |
| Other VPN (sessions) | 25 | | | |
| VPN Load Balancing | No Support | | | |
| **VPN Licenses** | | | | |
| Encryption | Base (DES) | *Opt. lic Strong (3DES/AES)* | | |
| Failover | Active/Standby (no stateful failover) | | | |
| Interfaces of all types, Max. | 120 | | | |
| Security Contexts | No Support | | | |
| Users, concurrent | 10 | *Optional licenses:* | 50 | Unlimited |
| VLANs/Zones, Maximum | Routed mode: 20<br><br>Transparent mode: 3 (2 regular zones and 1 failover link) | | | |
| VLAN Trunk, Maximum | 8 trunks | | | |

# ASA licencia

- Čo je z toho aktuálne podporované?
- **„show version“**

```
CCNAS-ASA# show version

<output omitted>

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Disabled       perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 12             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has a Base license.
```



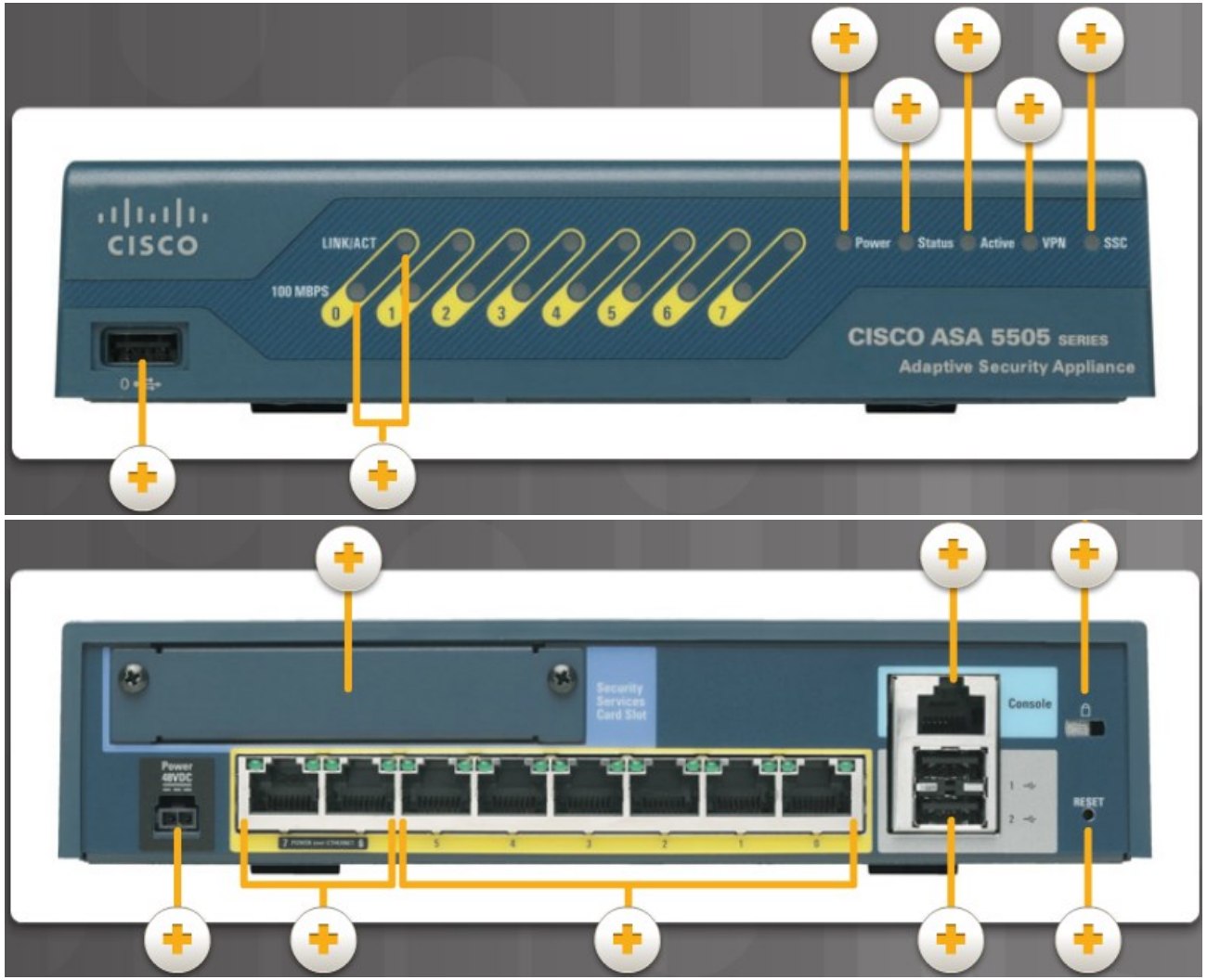
# Basic ASA Configuration

Kapitola sa zaoberá:

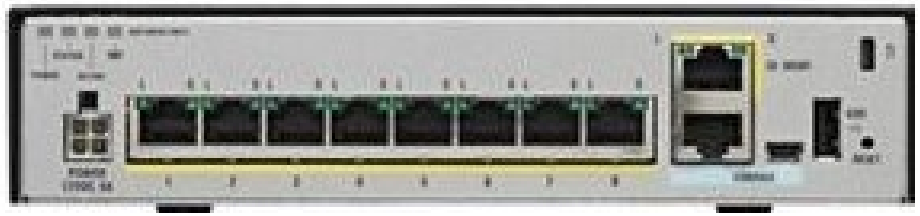
- ASA 5505
- ASA 5506-X
- ASA úrovne bezpečnosti
- Nasadenia ASA 5505

# Prehľad ASA 5505

- Male podniky, pobočky, teleworkers
  - EoS 2017, EoL 2022
  - Amazon (2020) od 60$ (refurb) po 280$ (nová)
  - Small edge appliance
- Podporuje
  - SSL VPN, IPsec VPN,
- DRAM 256 MB (rozšíriteľná na 512 MB)
- Flash pamäť 128 MB
- SSC slot
- 6 x Fast ethernet ports 10/100
- Serial Console Port
- 3 x 2.0 USB Ports
- Two PoE 10/100 Fast Ethernet Switch Ports
- Power Connector - 48 VDC power



# Prehľad ASA 5506-X with FirePOWER

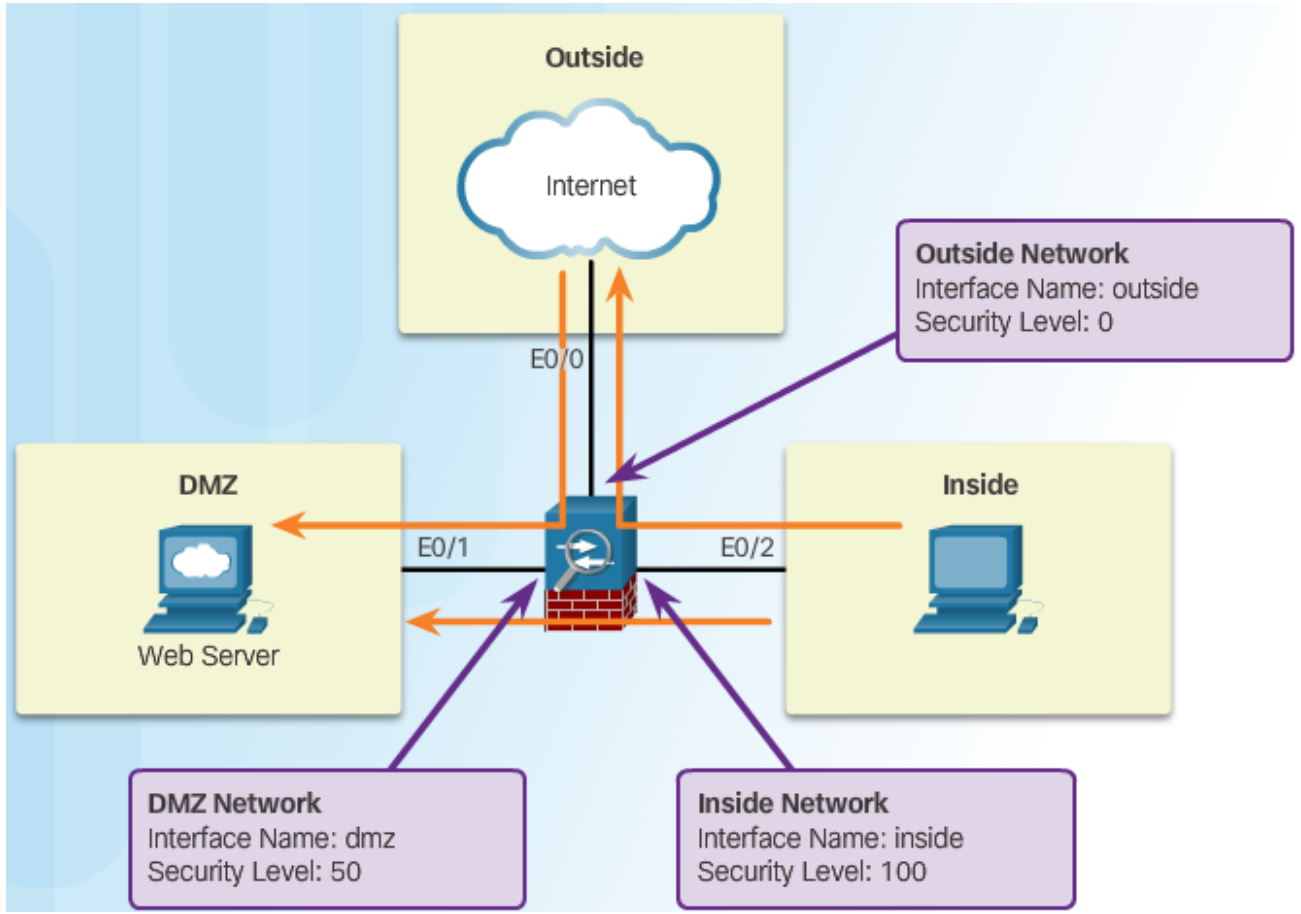
https://ciscogpl.com/
https://itprice.com/

- Amazon (2020): 350$, reál od 500 s Firepower cez 1200$
- DRAM 4GB
- 8 GB Flash pamäť
- mSATA Disk 50GB
- Nepoužíva SwitchPorts
- Crypto akcelerátor
- Power Connector - 12V
- Power, Status Active and wLAN LED
- 8 x 1 Gigabit Ethernet Ports (L – Link status, S – Connection status)
- Gigabit ethernet Management Port
- RJ45 Console port a mini USB Console Port
- Reset PIN
- USB typ A – disk musí mať formát FAT-32

# ASA - úrovne bezpečnosti

- Tzv. Security levels
  - Implementácia zónového FW
    - Odlíšenie Inside/outside/DMZ
- Úrovne zabezpečenia
  - Riadenie prístupu
    - Od 0 (nedôveryhodné)
      - Typicky Outside
    - Až 100 (veľmi dôveryhodné)
      - Typicky Inside
    - DMZ => medzi
  - Permit by default z vyššieho na nižšie a inšpekcia v obrátenom smere
  - Deny z nižšieho na vyššie

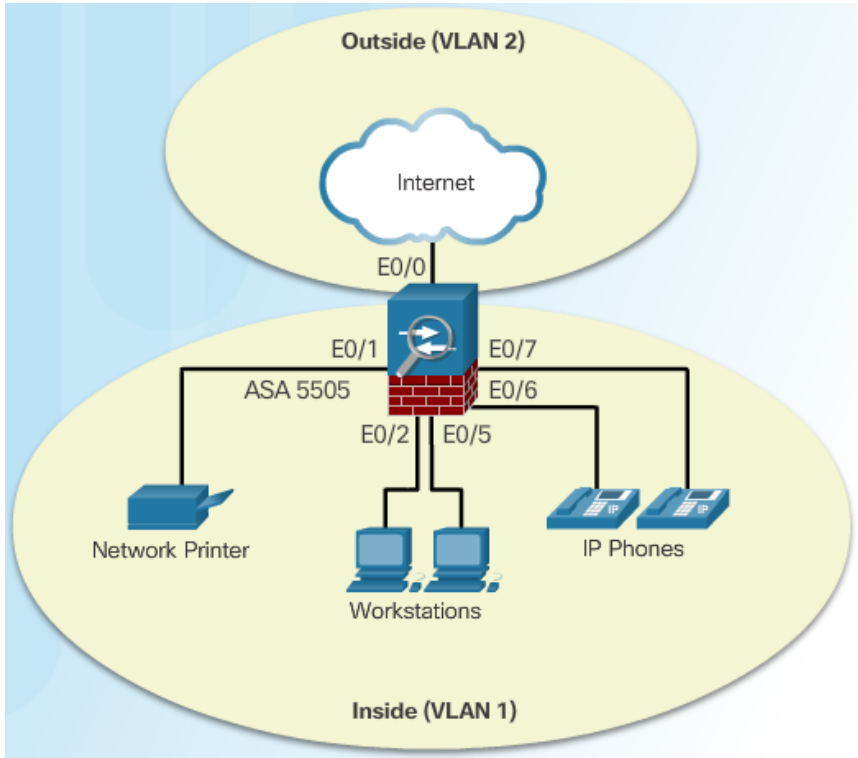
- Každé operačné rozhranie musí mať priradený názov a úroveň zabezpečenia
  - Aplikácia prísstupových rules



# Nasadenie ASA 5505

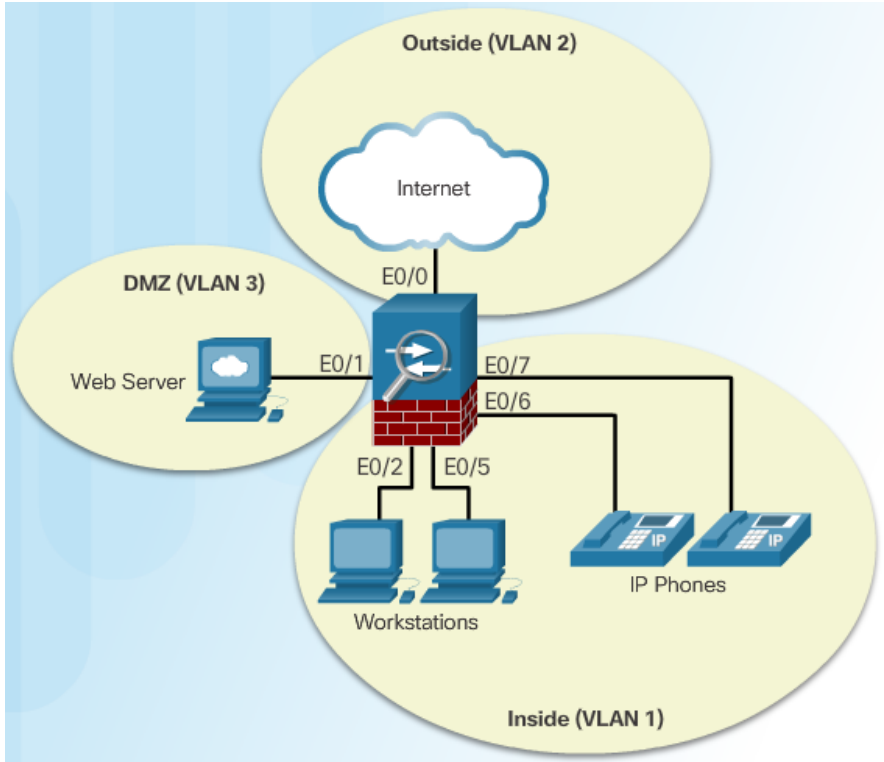
## Nasadenie ASA v malej pobočke

- Small edge device with PoE
- Medzi modem (DSL, cable) a sieť
- Dve zóny
  - Inside: Level 100
  - Outside: Level 0



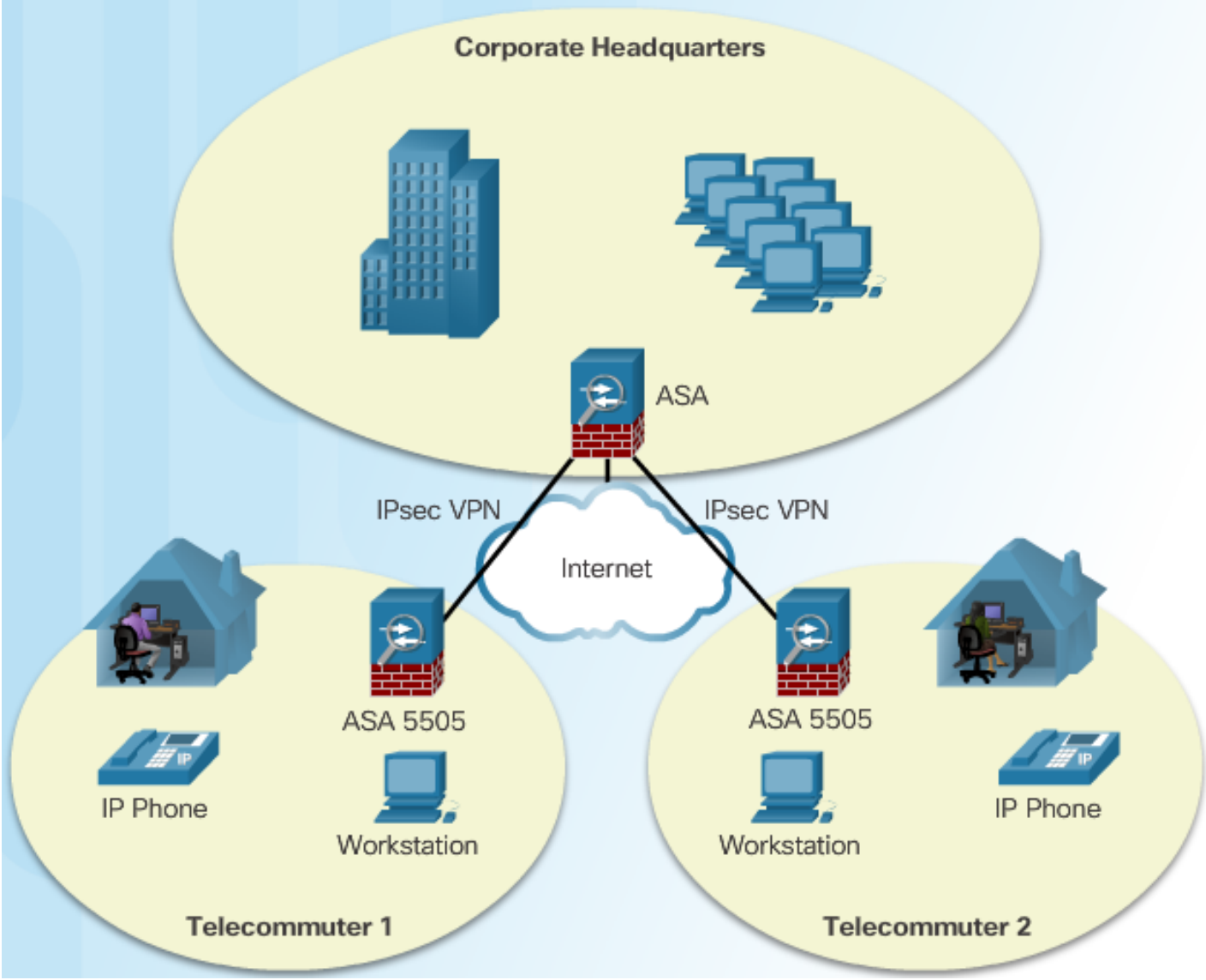

## Nasadenie ASA v malom podniku

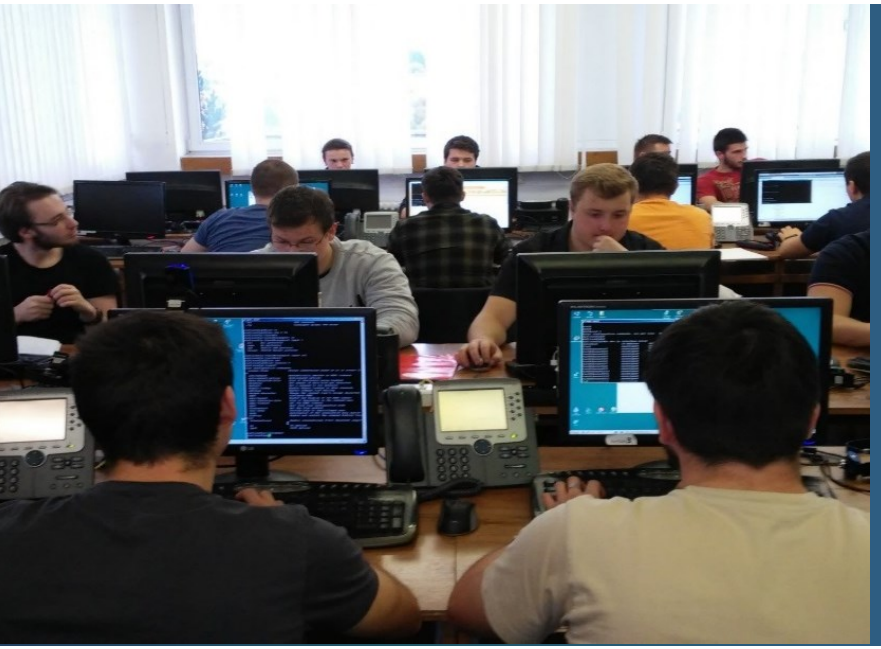
- „Klasický“ troj-zónový prístup



# Nasadenie ASA – podnik s pobočkami

- Tele/Home/Branch
- + riešenie site-to-site VPN na centrálu





# ASA Firewall Configuration

Kapitola sa zaoberá konfiguráciou:

- Firewallu ASA
- Manažmentových nastavení a služieb
- ACLs, služieb NAT na ASA
- Politiky služieb týkajúce sa ASA

# Konfigurácia ASA Firewallu

- ASA konfigurácia
  - Cez CLI
  - Cez ASDM GUI (Adaptive Security Device Manager)
- Rozhranie príkazového riadka ASA (CLI)
  - Patentovaný OS (nástupca PIX OS)
  - Ovládaním podobný ako CLI na Cisco smerovači, ale nie identický

- Rovnako ako IOS CLI aj ASA CLI rozpoznáva:
  - použitie príkazu (?)
  - použitie klávesy Tab
  - vykonanie čiastočného príkazu
  - pohyb medzi módmi (exit + end)

| IOS Router Command | Equivalent ASA Command |
|---|---|
| `enable secret` *password* | `enable password` *password* |
| `line vty 0 - 4`<br>`password` *password*<br>`login` | `passwd` *password* |
| `ip route` | `route` *if_name* |
| `show ip interfaces brief` | `show interfaces ip brief` |
| `show ip route` | `show route` |
| `show vlan` | `show switch vlan` |
| `show ip nat translations` | `show xlate` |
| `copy running-config startup-config` | `write [memory]` |
| `erase startup-config` | `write erase` |

# ASA CLI – základy

```
! pohyb v CLI a konfig mody
ciscoasa> e?

  enable    exit
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# exit
ciscoasa(config)# exit
ciscoasa#

! Show ide aj bez do a inde ako v EXEC
! Dopisovanie tiez
ciscoasa(config)# show runn<TAB>
ciscoasa(config)# show running-config

! Napoveda cez ?
ciscoasa(config)# show ?

exec mode commands/options:
  aaa                   Show information for AAA
runtime data
  aaa-server            Show aaa-server configuration
information
…
```

```
! Napoveda ina ako v IOS
ciscoasa(config)# help KEYWORD_OR_PRIKAZ
ciscoasa(config)# help interface

USAGE:

        interface
<type><type_id>[.<subif_number>]
        [no] interface
<physical_type><type_id>.<subif_number>
        [no] interface BVI <id>
        [no] interface
<dyn_type><type_id>[.<subif_number>]
        show running-config [all] interface
<type><type_id>[.<subif_number>]
        show interface {<type>
<type_id>[.<subif_number> | <if_name>}
        [detail|stats|ip brief|summary]
        clear config interface
{<type><type_id>[.<subif_number>]}
        clear interface
{<type><type_id>[.<subif_number>]}

DESCRIPTION:

interface       Set network interface parameters
                show/clear interface counters
                show brief summary of IP status
and configuration

SYNTAX:

<type>          <physical_type> | <dyn_type>
<type_id>       <phys_number> | <dyn_number>
<phys_number>   <port>|<slot>/<port>
```

# ASA - základná konfigurácia SVI

- HW ASA 5505
  - Dodávaná s predvolenou konfiguráciou
    - hostname, konfigurácia rozhraní (e0/0 - outside, e0/1 - e0/7 vo VLAN 1),
      DHCP služby...
  - Pomoc pri nasadení pre menej znalého používateľa
    - vo väčšine prípadov stačí pre SOHO nasadenie
- Konfigurácia obsahuje 2 predkonfigurované siete VLAN
  - VLAN 1 – pre vnútornú *INSIDE* sieť
  - VLAN 2 – pre vonkajšiu *OUTSIDE* sieť
- Všetky výrobné nastavenia je možné zmeniť
  - Manuálne pomocou príkazového riadku (CLI)
  - Interaktívne pomocou sprievodcu inicializácie nastavenia CLI
  - Použitím ASDM
- Resetovať ASA firewall do výrobných nastavení je možné príkazom *"configure factory-default"*

- Pozn. *Pozor, ASAv v GNS3 nie je prednastavená*

```
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!

        <output omitted>

interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute

        <output omitted>

object network obj_any
 nat (inside,outside) dynamic interface
        <output omitted>
http server enable
http 192.168.1.0 255.255.255.0 inside

        <output omitted>

dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside

        <output omitted>
```

# Sprievodca inicializácie nastavenia CLI

- Sprievodca (*wizard*) sa spustí po vymazaní a reštartovaní pomocou:
  - *"write erase"* a *"reload"*.
- Po dokončení interaktívnej konfigurácie sa zobrazí súhrn novej konfigurácie.
- Potvrdenie konfigurácie ju uloží na flash, alebo je možné túto konfiguráciu reštartovať a opraviť chybné nakonfigurované nastavenia.

```
Pre-configure Firewall now through interactive prompts [yes]? no



Type help or '?' for a list of available commands.
ciscoasa>
```

```
Pre-configure Firewall now through interactive prompts [yes]?
Firewall Mode [Routed]:
Enable password []: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2015]:
  Month [Mar]: April
  Day [29]: 1
  Time [18:06:03]: 12:00:00
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2

The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 12:00:00 April 1 2015
Firewall Mode: Routed
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2
```

# Manažmentové nastavenia a služieb

ASA CLI
Základná konfigurácia ASA (hostname, clock...)
VLANs
Telnet, SSH
NTP, DHCP

# Konfigurácia manažmantových nastavení a služieb

- Ak správca nevyužije možnosť interaktívnej konfigurácie, zobrazí sa ASA CLI.
- Pohyb v režioch ako v CLI
  - ***Enable, conf t, exit, end***
- Pre správne fungovanie ASA je potrebné nastaviť dátum a čas
  - manuálne: **clock set *HH:MM:SS Month Day Year***
  - automaticky: pomocou NTP servera
- Pri prvom otvorení konfiguračného režimu (***configure terminal***), sa zobrazí správa o funkcii *Smart Call Home*.
- Smart Call Home
  - proaktívna diagnostika
  - upozornenia v reálnom čase na vybraných cisco zariadeniach
  - vyššia dostupnosť siete
  - vyššia prevádzková efektívnosť
  - Nutnosť: ID cisco.com, ASA musí byť registrovaná na základe zmluvy o poskytovaní služieb Cisco SMARTnet.

# Konfigurácia základných nastavení a služieb

| ASA Command | Description |
|---|---|
| **hostname** *name* | • Specifies a hostname up to 63 characters.<br>• A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. |
| **domain-name** *name* | • Sets the default domain name. |
| **enable password** *password* | • Sets the enable password for privileged EXEC mode.<br>• Sets the password as a case-sensitive string of 3 to 32 alphanumeric and special characters (not including a question mark or a space). |
| **banner motd** *message* | • Provides legal notification and configures the system to display a message-of-the-day banner when connecting to the ASA. |
| **key config-key password-encryption** [ *new-pass* [ *old-pass* ]] | • Sets the passphrase between 8 and 128 character long.<br>• Used to generate the encryption key. |
| **password encryption aes** | • Enables password encryption and encrypts all user passwords. |

# Konfigurácia základných nastavení a služieb

```
! Odporúčaná základná konfigurácia ASA
ciscoasa(config)# hostname Moja-ASA
Moja-ASA(config)# domain-name kis.fri.uniza.sk
Moja-ASA(config)# enable password class
Moja-ASA(config)# banner motd
Moja-ASA(config)# banner motd VYSTRAHA! Toto je KIS
Moja-ASA(config)# banner motd #######
Moja-ASA(config)# banner motd #       # #####  ###### #    #   ##   #      #
Moja-ASA(config)# banner motd #       # #    # #      #    #  #  #  #      #
Moja-ASA(config)# banner motd #####   # #    # #####  #    # #    # #      #
Moja-ASA(config)# banner motd #       # #####  #      # ## # ###### #      #
Moja-ASA(config)# banner motd #       # #   #  #      ##  ## #    # #      #
Moja-ASA(config)# banner motd #       # #    # ###### #    # #    # ###### ######
Moja-ASA(config)# banner motd Neautorizovany vstup je trestny!

! Zapnutie silnejsieho sifrovania hesiel, default ND5
Moja-ASA(config)# show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
Moja-ASA(config)# key config-key password-encryption CISCO123
Moja-ASA(config)# password encryption aes
Moja-ASA# show password encryption
Password Encryption: Enabled
Master key hash: 0x57ba2069 0xde760f4b 0x99fe0d9d 0xecd2f686 0x5096446d(not saved)
Moja-ASA#
```

# Konfigurácia manažmantových nastavení a služieb

## ASA 5505

- 8 integrovaných prepínaných portov (layer 2) => nutnosť konfigurovať dva druhy rozhraní
  - **Buď Logické VLAN rozhranie**
    - Tieto rozhrania sú nakonfigurované ako layer 3 vrátane názvu, IP adresy a úrovne zabezpečenia.
  - **Alebo fyzické prepínacie porty**
    - Porty prepínača layer 2, ktoré sú priradené logickým rozhraniam VLAN

## Modely ASA 5500 vrátane ASAv

- Fyzickému portu môže byť priamo priradená IP adresa (layer 3)

# Konfigurácia manažmantových nastavení a služieb

- ASA 5505
  - Parametre 3 vrstvy sú konfigurované na logickom VLAN (SVI)
    - Vyžaduje sa: meno, úroveň zabezpečenia, IP adresu
  - Prepínané porty 2 vrstvy sú potom priradené konkrétnej VLAN.
    - Tieto porty môžu navzájom komunikovať pomocou hardvérového prepínania, ak sú v rovnakej VLAN.
  - Ak porty patria do rôznych VLAN, ASA aplikuje bezpečnostnú politiku na prenos a smerovanie medzi týmito VLAN-ami.
  - Pozn. Počet LVAN závisí od licencie
    - Basic ponúka len DVE

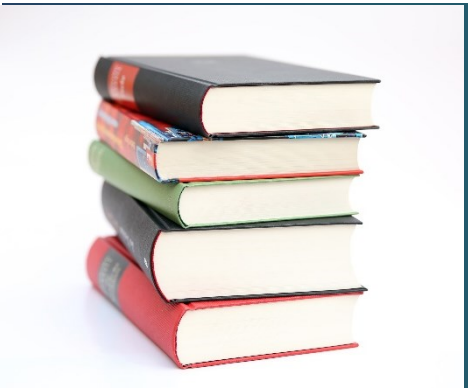
# Konfigurácia logických VLAN rozhraní

- Logické VLAN rozhrania musia byť pridelené pomocou príkazov
  - **`interface [vlan vlan-numbe`**
  - **`nameif [if_name]`**
  - **`security-level [value]`**

| ASA Command | Description |
|---|---|
| `interface vlan vlan-number` | • Enters VLAN interface configuration mode. |
| `nameif if_name` | • Names the interface using a text string of up to 48 characters.<br>• The name is not case-sensitive.<br>• You can change the name by re-entering this command with a new value.<br>• Do not enter the no form, because that command causes all commands that refer to that name to be deleted. |
| `security-level value` | • Sets the security level, where number is an integer between 0 (lowest) and 100 (highest). |

- Konfigurácia IP adresy rozhrania
  - Manuálne
  - DHCP
  - PPPoE

| To Configure | ASA Command | Description |
|---|---|---|
| Manually | `ip address ip-address netmask` | • Assigns an IP address to the interface. |
| Using DHCP | `ip address dhcp` | • Used to have the interface request an IP address configuration from the upstream device. |
| | `ip address dhcp setroute` | • Used to have the interface request and install a default route to the upstream device. |
| Using PPP0E | `ip address pppoe` | • Interface configuration mode command that requests an IP address from the upstream device. |
| | `ip address pppoe setroute` | • Same command but it also requests and installs a default route to the upstream device. |



# FUN FACT – ASA 5505

- ASA 5505 so základnou licenciou neumožňuje vytvorenie troch plne funkčných VLAN rozhraní.
- Je možné vytvoriť tretie VLAN rozhranie, ktoré bude obmedzené avšak je nutné dodržať
  - Ak je najprv nakonfigurované príkazom: ***no forward interface vlan*** *[number]*
    - Tento príkaz obmedzuje toto rozhranie pri nadviazaní kontaktu s inou VLAN.
  - Ak sú nakonfigurované vnútorné a vonkajšie VLAN rozhrania, príkaz ***no forward interface vlan*** *[number]* musí byť zadaný pred príkazom ***nameif*** na treťom rozhraní.
- Parameter *[number]* určuje ID VLAN-y, ku ktorému toto rozhranie nemôže iniciovať prenos.
- Riešením tohto problému, a dosiahnutie úplnej funkčnosti, je kúpa licencie Security Plus.

# Konfigurácia portov druhej vrstvy a statickej cesty

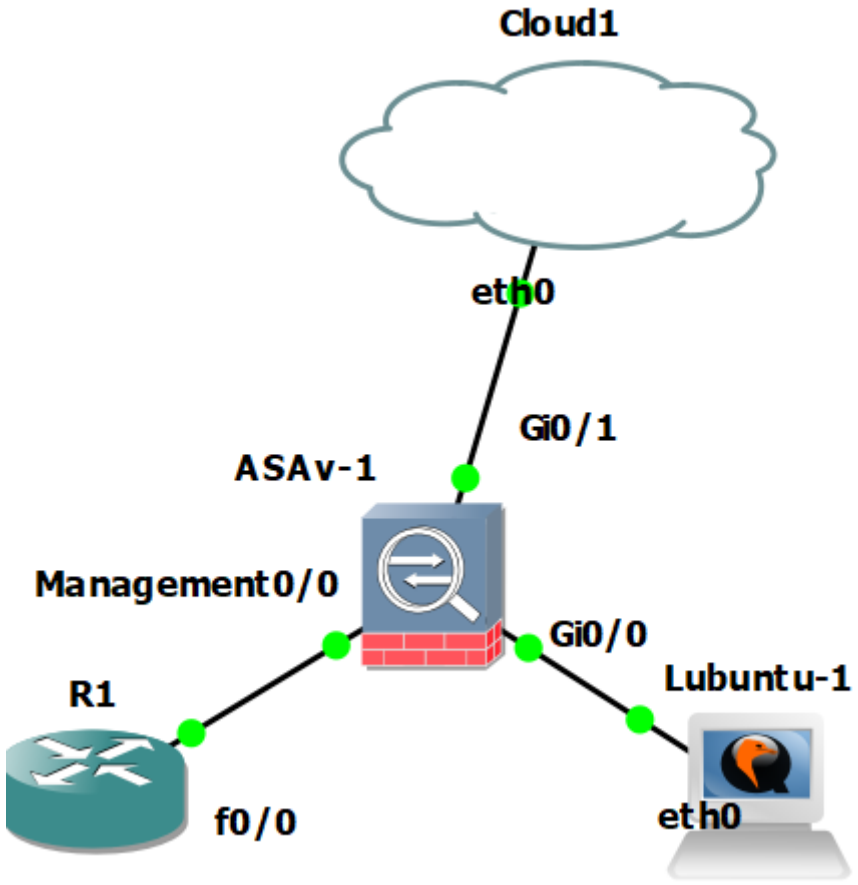
- Predvolené nastavenia
  - Všetky prepínacie porty druhej vrstvy sú vo VLAN 1.
- Zmena predvolených nastavení

```
Inter e0/0
   switchport access vlan [vlan_id]
   no shutdown
```

- Overenie
  - **show switch vlan** – overenie nastavení VLAN
  - **show interface ip brief** – zobrazenie stavu všetkých rozhraní
  - **show ip address** – zobrazenie informácií pre VLAN rozhrania tretej vrstvy (layer 3)
- Predvolená statická cesta (Default static route)
  - Ak je ASA nakonfigurovaná ako DHCP klient, predvolenú statickú cestu sa môže naučiť z upstrem zariadenia.
  - V opačnom prípade sa konfiguruje manuálne

```
route [interface-name] 0.0.0.0 0.0.0.0 [next-hop-ip-address]
show route
```

# Konfigurácia L3 portov - ASAv




```
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.1
255.255.255.0
!
interface Management0/0
 nameif MGMT
 security-level 100
 ip address 192.168.1.1
255.255.255.0
!
```

# Konfig DHCP client a overenie

```
! IF ako Dhcp client v GKR
dhcpd auto_config IF_NAME

! Priklad
Moja-ASA(config)# int gi 0/1
Moja-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
Moja-ASA(config-if)# ip address dhcp

Moja-ASA(config-if)# sh int ip brie
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.2.1     YES manual up                    up
GigabitEthernet0/1         158.193.152.118 YES DHCP   up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
GigabitEthernet0/4         unassigned      YES unset  administratively down down
GigabitEthernet0/5         unassigned      YES unset  administratively down down
GigabitEthernet0/6         unassigned      YES unset  administratively down down
Management0/0              192.168.1.1     YES manual up                    up
```

# Konfig default route a overenie

```
Moja-ASA(config)# route outside 0.0.0.0 0.0.0.0 ?

configure mode commands/options:
  Hostname or A.B.C.D  The address of the gateway by which the foreign network
                       is reached.
Moja-ASA(config)# route outside 0.0.0.0 0.0.0.0 158.193.152.1
Moja-ASA(config)# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 158.193.152.1 to network 0.0.0.0

S*        0.0.0.0 0.0.0.0 [1/0] via 158.193.152.1, outside
C         158.193.152.0 255.255.255.128 is directly connected, outside
L         158.193.152.118 255.255.255.255 is directly connected, outside
C         192.168.1.0 255.255.255.0 is directly connected, MGMT
L         192.168.1.1 255.255.255.255 is directly connected, MGMT
C         192.168.2.0 255.255.255.0 is directly connected, inside
L         192.168.2.1 255.255.255.255 is directly connected, inside

Moja-ASA(config)# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 ms
Moja-ASA(config)#
```

# Konfigurácia DHCP servera

| ASA Command | Description |
|---|---|
| `dhcpd address IP_address1 [-IP_address2 ] if_name` | • Creates a DHCP address pool in which IP_address1 is the start of the pool and IP_address2 is the end of the pool, separated by a hyphen.<br>• The address pool must be on the same subnet as the ASA interface. |
| `dhcpd dns dns1 [dns2 ]` | • (Optional) Specifies the IP address(es) of the DNS server(s). |
| `dhcpd lease lease_length` | • (Optional) Changes the lease length granted to the client which is the amount of time in seconds that the client can use its allocated IP address before the lease expires.<br>• The lease_length defaults to 3600 seconds (1 hour) but can be a value from 0 to 1,048,575 seconds. |
| `dhcpd domain domain_name` | • (Optional) Specifies the domain name assigned to the client. |
| `dhcpd enable if_name` | • Enables the DHCP server service (daemon) on the interface (typically the inside interface) of the ASA. |

```
! ASA ako DHCP server, 5505 s BASE max 32 adries
dhcpd address 192.168.2.2-192.168.2.32 inside
dhcpd dns 8.8.8.8 1.1.1.1
dhcpd lease 3600
dhcpd domain kis.fri.uniza.sk
dhcpd enable inside

! Nastav pre DHCP server DNS, WINS, Domain name ako
! sa naucil ASA int so spustenym DHCP client-om
dhcpd auto_config outside
```

# Overenie DHCP servera

```
Moja-ASA# sh dhcpd state
Context  Configured as DHCP Server
Interface MGMT, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER

Moja-ASA# show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

    192.168.2.2    010c.ea0f.5fd2.00            3560 seconds    Automatic

Moja-ASA# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools         1
Automatic bindings    1
Expired bindings      0
Malformed messages    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          2
DHCPREQUEST           3
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             2
DHCPACK               2
DHCPNAK               1
```

# Konfigurácia vzdialeného prístupu - SSH

```
Moja-ASA(config)# username admin password cisco123
Moja-ASA(config)# aaa authentication ssh console LOCAL
Moja-ASA(config)# crypto key generate rsa modulus 768
Moja-ASA(config)# ssh version 2
! Povol SSH z Ipciek vstupujucich cez rozhranie
Moja-ASA(config)# ssh 192.168.1.0 255.255.255.0 MGMT
! Ine rozhranie
! ssh 192.168.100.0 255.255.255.0 inside

! overenie
Moja-ASA(config)# show ssh
Idle Timeout: 5 minutes
Version allowed: 2
Cipher encryption algorithms enabled:    aes128-cbc   aes192-cbc   aes256-cbc
aes128-ctr   aes192-ctr   aes256-ctr
Cipher integrity  algorithms enabled:    hmac-sha1    hmac-sha1-96

Hosts allowed to ssh into the system:
192.168.1.0 255.255.255.0 MGMT
Moja-ASA(config)#
```

# Konfigurácia vzdialeného prístupu - telnet

```
! Prepokladajme Ipcka uz je
! kurikulum uvadza, na ASAv nejde
Moja-ASA(config)# password Cisco
Moja-ASA(config)# telnet 192.168.1.0 255.255.255.0 MGMT
Moja-ASA(config)# telnet timeout 3
Moja-ASA(config)# Show run telnet

! ASAv + odporucam pouzivat v GNS3
Moja-ASA(config)# username admin password cisco123
Moja-ASA(config)# aaa authentication telnet console LOCAL
! Povol telnet z Ipciek vstupujucich cez rozhranie
Moja-ASA(config)# telnet 192.168.1.0 255.255.255.0 MGMT
! Ine rozhranie
! telnet 192.168.100.0 255.255.255.0 inside
Moja-ASA# show run telnet
telnet 192.168.1.0 255.255.255.0 MGMT
telnet timeout 5
Moja-ASA(config)#
```

# Konfigurácia DNS a overenie

```
! povol dns lookup na danych rozhraniach
Moja-ASA(config)# dns domain-lookup outside
Moja-ASA(config)# dns domain-lookup inside
Moja-ASA(config)# dns name-server 8.8.8.8

!overenie
Moja-ASA(config)# ping netacad.uniza.sk
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 158.193.152.8, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 1/1/1 ms
Moja-ASA(config)#
```

# Konfigurácia NTP

| ASA Command | Description |
|---|---|
| `ntp authenticate` | • Enables authentication with an NTP server. |
| `ntp trusted-key key_id` | • Specifies an authentication key ID to be a trusted key, which is required for authentication with an NTP server. |
| `ntp authentication-key key_id md5 key` | • Sets a key to authenticate with an NTP server. |
| `ntp server ip_address [key key_id]` | • Identifies an NTP server. |

```
! Autentifikovana NTP sluzba
! Ntp kluc a heslo musi byt aj na NTP servery
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 Cisco123
ntp server 1.1.1.1
```

# NTP príklad SVK a overenie

```
! 2.sk.pool.ntp.org a 0.europe.pool.ntp.org bez AUTH
ntp server 90.176.21.0 prefer
ntp server 45.148.141.154

!overenie
Moja-ASA# show ntp associations
      address         ref clock      st  when  poll reach  delay  offset
disp
 ~90.176.21.0      .PPS.             1    54    64    0      9.9  148.92
16000.
 ~45.148.141.154   0.0.0.0          16     -    64    0      0.0    0.00
16000.
 * master (synced), # master (unsynced), + selected, - candidate, ~
configured
Moja-ASA# show ntp status
Clock is synchronized, stratum 2, reference is 90.176.21.0
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is e36cfec1.81466a5d (16:52:17.504 UTC Sat Nov 28 2020)
clock offset is -0.7027 msec, root delay is 9.63 msec
root dispersion is 15892.35 msec, peer dispersion is 15890.63 msec
```


# Objekty a objektové skupiny (Objects and Object Groups)

Network objects

Service objects

Object groups

# Čo sú objekty a objektové skupiny?

- Objekty sa vytvárajú a využívajú v ACL namiesto IP adries alebo protokolu/portu
  - Mnemo dôvody pre prácu s ACL
  - Jednoduchšia úprava ACL či iných konfigurácii
    - Pri úprave objektu sa zmena automaticky použije na všetky pravidlá, ktoré používa daný objekt
- Existujú 2 typy objektov
  - Network object - konfiguruje sa pomocou príkazu: **object network**
    - Môže byť troch typov: **host, podsieť alebo rozsah**
      - konkrétna IP adresa, celá podsieť, rozsahom adries
  - Service object - konfiguruje sa pomocou príkazu: **object service**
    - Obsahuje protokol a voliteľný zdrojový a/alebo cieľový port, či rozsah portov
- Objekty môžu byť v prípade potreby pripojené alebo odobraté od jednej alebo viacerých skupín objektov.
- Jednotlivé objekty môžu byť využité pri NAT, ACL a objektových skupinách.

# Konfigurácia sieťového objektu (Network object)

- Sieťový objekt (**Network object**):
  - názov objektu obsahuje iba jednu IP adresu/rozsah a masku
  - v sieťovom objekte preto môže byť len jeden príkaz
    - pri zadaní druhého páru IP adresy a masky sa nahradí existujúca konfigurácia
  - Môže byť definovaný jednou z troch metód

| ASA Command | Description |
|---|---|
| **host** *ip-addr* | • Assigns an IP address to the named object. |
| **subnet** *net-address net-mask* | • Assigns a network subnet to the named object. |
| **range** *ip-addr-1 ip-addr-n* | • Assigns a range of IP addresses to the named object |

  - príkazom - ***clear config object network*** - sa vymažú všetky sieťové objekty

# Sieťové objekty

```
!jedna IPcka
Moja-ASA(config)# object network ?

configure mode commands/options:
  WORD < 129 char  Specifies object ID
Moja-ASA(config)# object network INSIDE_IF
Moja-ASA(config-network-object)# host 192.168.2.1
Moja-ASA(config-network-object)# exit

! Range
Moja-ASA(config)# object network SIET_INSIDE
Moja-ASA(config-network-object)# range ?
network-object mode commands/options:
  A.B.C.D      Enter start IP address
  X:X:X:X::X   Enter start IPv6 address
Moja-ASA(config-network-object)# range 192.168.2.1 192.168.2.254

! overenie
Moja-ASA(config-network-object)# show runn object
object network INSIDE_IF
 host 192.168.2.1
object network SIET_INSIDE
 range 192.168.2.1 192.168.2.254
Moja-ASA(config-network-object)#
```

# Konfigurácia objektu služby (Service object)

- Objekt služby (**Service object**)
  - môže obsahovať port protokolu alebo rozsahy portov (ICMP, TCP, UDP...)
  - voliteľné kľúčové slová sa používajú na identifikáciu zdrojového alebo cieľového portu (alebo oboch).
  - Operátory: **eq**(equal), **neq**(not equal), **lt**(less than), **gt**(greater than) a **range** podporujú konfiguráciu portu pre daný protokol.
    - Ak nie je špecifikovaný operátor, predvolený je eq(equal).
  - príkazom - ***clear config object service*** – sa vymažú všetky servisné objekty

| ASA Command | Description |
|---|---|
| `service protocol [ source [ operator port ]] [ destination [ operator port ]]` | • Specifies an IP protocol name or number. |
| `service tcp [ source [ operator port ]] [ destination [ operator port ]]` | • Specifies that the service object is for the TCP protocol. |
| `service udp [ source [ operator port ]] [ destination [ operator port ]]` | • Specifies that the service object is for the UDP protocol. |
| `service icmp icmp-type` | • Specifies that the service object is for the ICMP protocol. |
| `service icmp6 icmp6-type` | • Specifies that the service object is for the ICMPv6 protocol. |

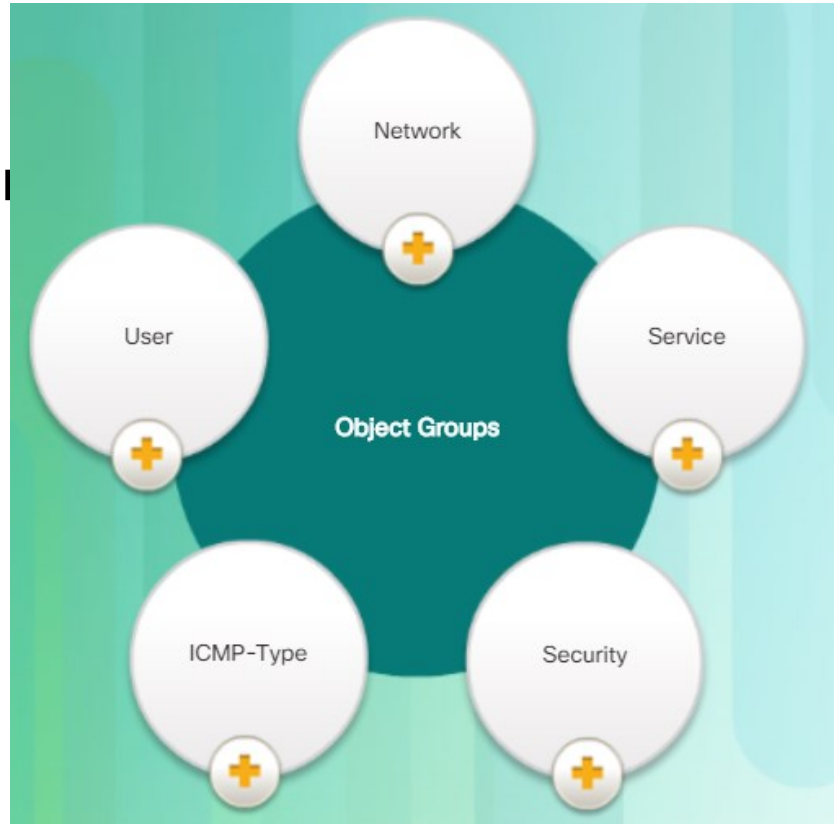
# Service object – príklad WWW

```
Moja-ASA(config)# object service HTTP
Moja-ASA(config-service-object)# service ?

service-object mode commands/options:
  <0-255>  Enter protocol number (0 - 255)
  ah
  eigrp
  esp
  gre
  icmp
  icmp6
  igmp
  igrp
  ip
  ipinip
  ipsec
  nos
  ospf
  pcp
  pim
  pptp
  sctp
  snp
  tcp
  udp

<--- More --->
```

```
Moja-ASA(config)# object service HTTP
Moja-ASA(config-service-object)# service tcp ?

service-object mode commands/options:
  destination  Keyword to specify destination
  source       Keyword to specify source
  <cr>
Moja-ASA(config-service-object)# service tcp
destination ?

service-object mode commands/options:
  eq      Port equal to operator
  gt      Port greater than  operator
  lt      Port less than operator
  neq     Port not equal to operator
  range   Port range operator
Moja-ASA(config-service-object)# service tcp
destination eq 80

! overenie
sh run object service
object service HTTP
 service tcp destination eq www
```

# Skupiny objektov (Object groups)

- Samotné objekty môžu byť zoskupené do pomenovanej skupiny
- Zoskupením podobných objektov sa dá skupina použiť v zázname riadenia prístupu (ACE – access control entry) namiesto toho, aby bolo nutné zadávať ACE pre každý objekt osobitne.
- ASA podporuje rôzne typy objektových skupín
  - network, service, protocol, security, ICMP-Type, user
- Pre objektové skupiny platí:
  - objekty a objektové skupiny zdieľajú rovnaký priestor mien
  - objektové skupiny musia mať jedinečné názvy
  - objektovú skupinu nemožno odstrániť alebo vyprázdniť, ak sa použije v príkaze
  - ASA nepodporuje skupiny vnorených skupín IPv6



# Konfigurácia všeobecných objektových skupín

- **Network object group**
  - konfigurácia pomocou príkazu ***object-group network*** *[grp-name]*
  - *v konfiguračnom režime skupiny pomocou príkazov* ***network-object*** *a* ***group-object*** *pridáme sieťové objekt*

```
Moja-ASA(config)# object-group network ADMIN_HOSTS
Moja-ASA(config-network-object-group)# description Stroje Adminov
! Umoznuje kombinovat IPv4 aj IPv4
Moja-ASA(config-network-object-group)# network-object host 192.168.2.50
Moja-ASA(config-network-object-group)# network-object host 2001:ACAD:FFFF::50

Moja-ASA(config)# object network SSH_JUMP_IN
Moja-ASA(config-network-object)# host 192.168.2.2
Moja-ASA(config-network-object)# exit

Moja-ASA(config)# object-group network SSH_SERVERY
Moja-ASA(config-network-object-group)# description ZOZNAM SSH SERVEROV
Moja-ASA(config-network-object-group)# network-object host 192.168.2.4
! Odvolavat sa na vytvoreny network object
Moja-ASA(config-network-object-group)# network-object object SSH_JUMP_IN
```

# Overenie

```
Moja-ASA# sh run object-group
object-group network ADMIN_HOSTS
 description Stroje Adminov
 network-object host 192.168.2.50
 network-object host 200:acad:ffff::55
object-group network SSH_SERVERY
 description ZOZNAM SSH SERVEROV
 network-object host 192.168.2.4
 network-object object SSH_JUMP_IN
```

# Konfigurácia všeobecných objektových skupín

- **ICMP-Type object group**
  - konfigurácia príkazom ***object-group icmp-type*** *[grp-name]*
  - *na pridanie objektov do skupiny použijeme príkazy* ***icmp-object*** a ***group-object***

```
CCNAS-ASA(config)# object-group icmp-type ICMP-ALLOWED
CCNAS-ASA(config-icmp-object-group)# icmp-object echo
CCNAS-ASA(config-icmp-object-group)# icmp-object time-exceeded
CCNAS-ASA(config-icmp-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object-group id ICMP-ALLOWED
object-group icmp-type ICMP-ALLOWED
 icmp-object echo
 icmp-object time-exceeded
CCNAS-ASA(config)#
```

# Konfigurácia všeobecných objektových skupín

- **Service object group**
  - konfigurácia - ***object-group service*** *[grp-name]*
  - *pridávanie objektov* - ***port-object*** a ***group-object***

- Na odstránenie všetkých skupín objektov z konfigurácie slúži príkaz
  - ***clear configure object-group***

- Overenie
  - ***show running-config object-group***

```
CCNAS-ASA(config)# object-group service SERVICES-1
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq www
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq https
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq pop3
CCNAS-ASA(config-service-object-group)# service-object udp destination eq ntp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-2 tcp
CCNAS-ASA(config-service-object-group)# port-object eq www
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-3 tcp
CCNAS-ASA(config-service-object-group)# group-object SERVICES-2
CCNAS-ASA(config-service-object-group)# port-object eq ftp
CCNAS-ASA(config-service-object-group)# port-object range 2000 2005
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
```


# ACLs

ASA ACLs

Typy ASA ACLs

Konfigurácia a nasadenie ACLs

ACL a objektové skupiny

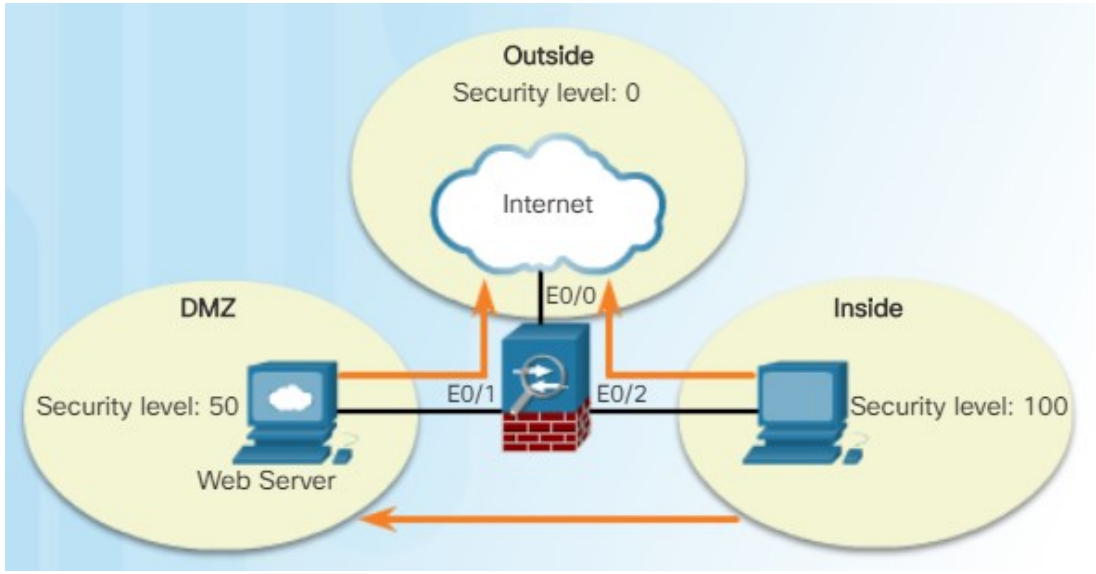
# ASA Acls

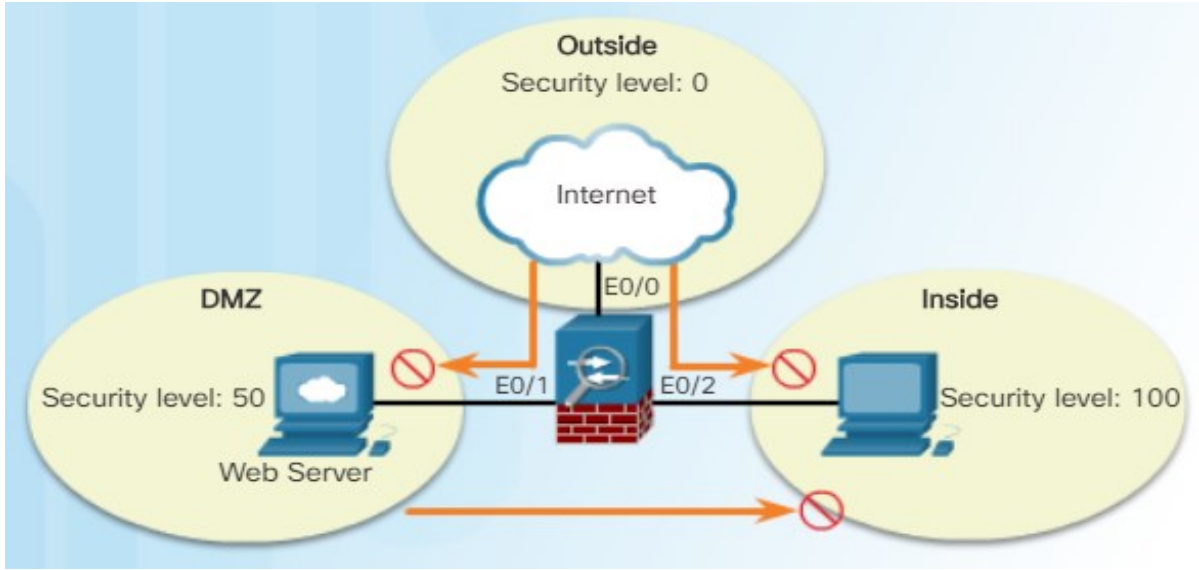
- Cisco ASA 5505 podporuje a poskytuje základné možnosti filtrovania
- **Zhody IOS ACL s ASA  ACL**
  - Obidve sú tvorené ACE
  - Spracúvajú sa postupne (zhora nadol)
  - Posledné pravidlo je implicitné deny
  - Platí pravidlo jedného ACL na rozhranie, protokol a na smer
- Odlišnosti ASA ACL
  - Namiesto wilcard masky (0.0.0.255) sa využíva sieťová maska (255.255.255.0)
  - Väčšina ASA ACLs je pomenovaná, nie číslovaná
  - Zabezpečenie rozhrania bez nakonfigurovaného ACL sa riadi na základe security level
  - Môže používať object-y a object-group-y, či identity namiesto IP adries

# Typy filtrovania ASA ACLs

- **Through-traffic filtering (Filtrovanie prenášaných paketov)**
  - prevádzka, ktorá prechádza zariadením  z jedného rozhrania do druhého
  - konfigurácia v 2 krokoch
    - vytvorenie ACL
    - aplikovanie vytvoreného ACL na rozhranie
- **To-the-box-traffic filtering (Filtrovanie paketov na zariadení)**
  - vzťahuje sa na filtrovanie prevádzky, ktorá končí na ASA
  - dostupné od verzie 8.0
  - konfigurácia je jednokroková, ale implementácia ma súbor pravidiel

# Vplyv *security-level* na filtrovanie




- Prevádzka z bezpečnejšieho rozhrania, napr. security level (SL) 100, má povolený prístup k menej bezpečným rozhraniam, napr. security level 0
  - Späť povolená na základe stavovej inšpekcie
- Prevádzka z nižšieho SL na vyšší SL
  - Je blokovaná
  - Je potrebné aplikovať ACL, ktoré umožňuje prenos z nižšej úrovne zabezpečenia do vyššej.
- Prevádzka medzi rozhraniami s rovnakými SL
  - Povolenie vyžaduje príkaz:

```
same-security-traffic permit inter-interface
```

  - Pre to isté rozhranie

```
same-security-traffic permit intra-interface
```

# Päť typov ASA ACL

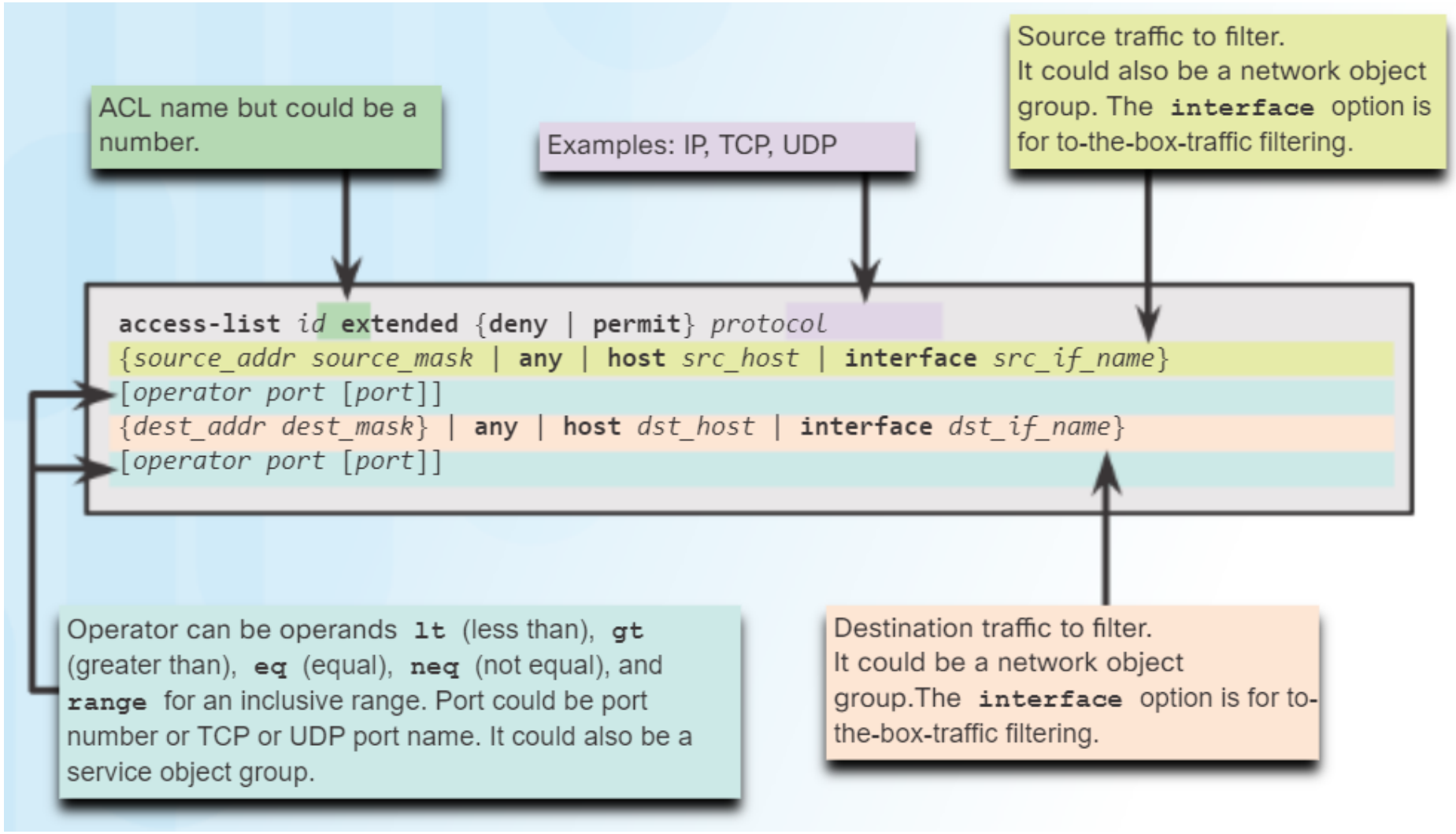
- **Extended access list**
  - Najbežnejší typ ACL, filtrovanie tak ako v IOS
- **Standard access list**
  - Na rozdiel od  IOS ACL kontroluje cieľové IP adresy
  - Zvyčajne sa využívajú v route mapách pri redistribúcií OSPF
  - Nemožno ich aplikovať na rozhranie na riadenie prístupu
- **EtherType access list**
  - Je ich možné konfigurovať iba ak je zariadenie spustené v transparentnom móde (transparent mode)
- **Webtype access list**
  - Používa sa v konfiguráciách, ktoré podporuje filtrovanie pre klientov SSL VPN.
- **IPv6 access list**
  - Používa sa na určenie prenosu, ktorý sa má blokovať a ktorá preposlať ďalej cez rozhranie.

# Konfigurácia ACLs

- Pomocný príkaz pri tvorbe ACL
  - ***help access-list***

| Element | Description |
|---|---|
| ACL id | • The name of the ACL. It can be any alphanumeric name up to 241 characters. |
| Action | • Can be **permit** or **deny**. |
| Protocol number - Source | • Can be **ip** for all traffic, or the name / IP protocol number (0-250) including **icmp** (1), **tcp** (6), **udp** (17), or a protocol object-group. |
| Source | • Identifies the source and can be **any**, a **host**, a network, or a network object group.<br>• For to-the-box-traffic filtering, the **interface** keyword is used to specify the source interface of the ASA. |
| Source port operator | • (Optional) Operand is used in conjunction with the source port.<br>• Valid operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** for an inclusive range. |
| Source port | • (Optional) Can be the actual TCP or UDP port number, select port name, or service object group. |
| Destination | • Identifies the destination and like the source, it can be **any**, a **host**, a network, or a network object group.<br>• For to-the-box-traffic filtering, the **interface** keyword is used to specify the destination interface of the ASA. |
| Destination port operator | • (Optional) Operand is used in conjunction with the destination port.<br>• Valid operands are the same as the source port operands. |
| Destination port | • (Optional) Can be the actual TCP or UDP port number, select port name, or service object group. |
| Log | • Can set elements for syslog including severity level and log interval. |
| Time range | • (Optional) Specify a time range for this ACE. |

# Príklad pre Extended ACL



# Implementácia ACLs

```
access-list ACL-IN extended deny tcp any host 209.165.201.29 eq www
access-list ACL-IN extended permit ip any any
access-group ACL-IN in interface inside
```

- ACL prevents all inside hosts access to a web service at 209.165.201.29.
- Internal hosts are permitted to access all other services at 209.165.201.29.
- Internal hosts are permitted access to all other addresses.
- All other traffic is implicitly denied.

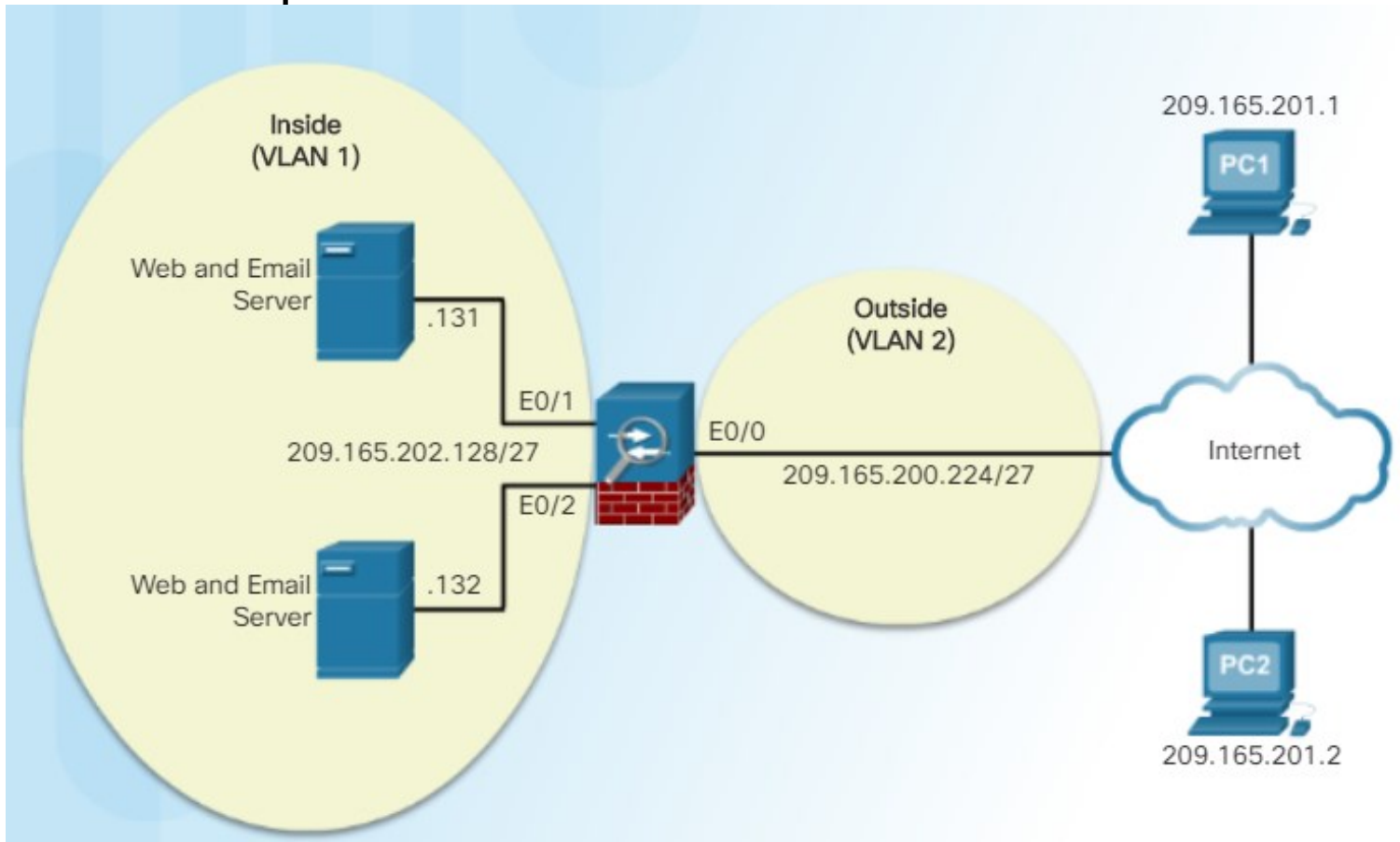
- Overenie
  - ***show access-list***
  - ***show running-config access-list***
- Vymazanie vytvoreného ACL
  - ***clear configure access-list***

```
access-group id { in | out } interface if_name [ per-user-override | control-plane ]
```

| Syntax | Description |
|---|---|
| **access-group** | Keyword used to apply an ACL to an interface. |
| *id* | The name of the actual ACL to be applied to an interface. |
| **in** | The ACL will filter inbound packets. |
| **out** | The ACL will filter outbound packets. |
| **interface** | Keyword to specify the interface to which to apply the ACL. |
| *if_name* | The name of the interface to which to apply an ACL. |
| **per-user-override** | Option that allows downloadable ACLs to override the entries on the interface ACL. |
| **control-plane** | Keyword to specify whether the applied ACL analyzes traffic destined to ASA for management purposes. |

# ACL a Objekty či Objektové skupiny

- Príklad
  - Z PC1 a PC2 povoľ prístup k webovým a e-mailovým službám vo vnútri
  - Všetko ostatné dropni



# ACLs pre PC1 a PC2 – klasický prístup

```
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-2 -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-2 -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
```

# Využitie objektových skupín pri ACL

```
access-list id extended { deny | permit } protocol object-group
network-obj-grp-id object-group network-obj-grp-id object-group
service-obj-grp-id
```

```
CCNAS-ASA(config)# object-group network NET-HOSTS
CCNAS-ASA(config-network-object-group)# description OG matches PC-A and PC-B
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.1
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.2
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network SERVERS
CCNAS-ASA(config-network-object-group)# description OG matches Web / Email Servers
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.131
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.132
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service HTTP-SMTP tcp
CCNAS-ASA(config-service-object-group)# description OG matches SMTP / WEB traffic
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# port-object eq www
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers
CCNAS-ASA(config)#  access-list ACL-IN extended permit tcp object-group NET-HOSTS
object-group SERVERS object-group HTTP-SMTP
```

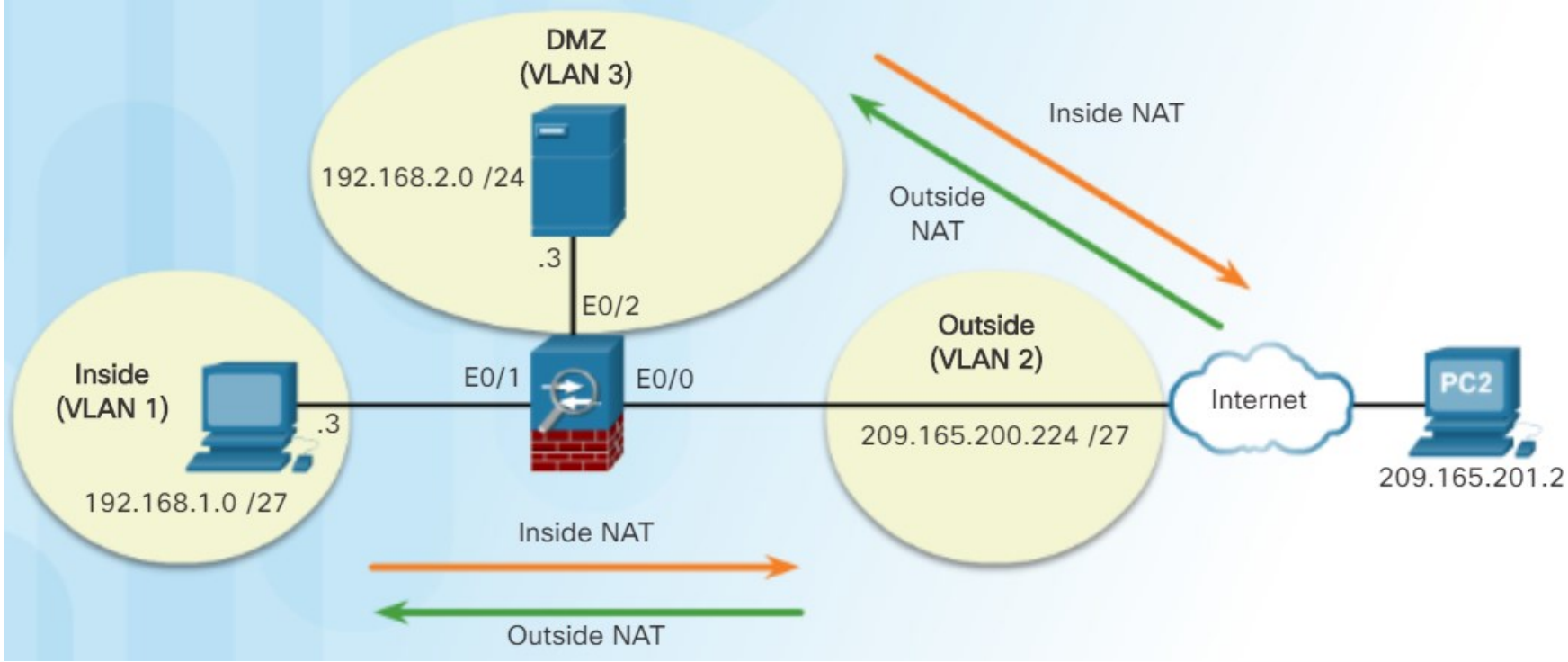

# NAT services on an ASA

Dynamic NAT

Dynamic PAT

Static NAT

# ASA NAT – nasadenie



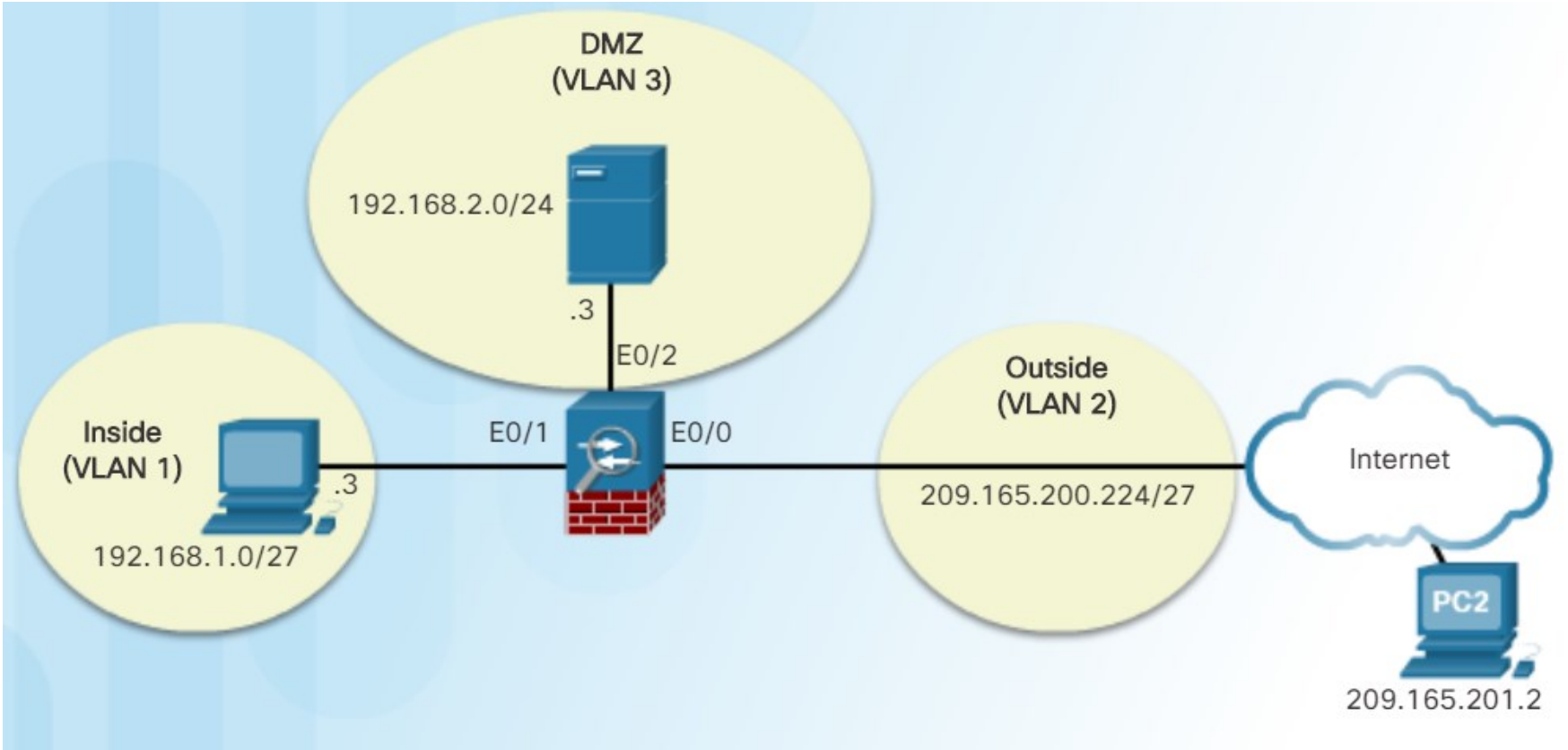

- Inside NAT
  - To najbežnejšie nasadenie
  - Z inside s vyšším SecLEvel na Outside s nižším SecLevel
  - Typicky prekladám najprv source
  - Najprv sa NAT-uje, potom sa smeruje
- Outside NAT
  - Preklad pri prechode z outside s nižším SecLevel na interface z vyšším SecLevel
  - Riešene kedy outside host sa javí ako člen vnútornej siete
  - Typicky prekladám najprv destiantion
  - Najprv sa smeruje, potom sa NAT-uje
- Bidirectional NAT
  - Keď sa používajú oba predchodzie typy
- Pozn. spôsob ovplyvňuje procesy ako kedy sa robí NAT a kedy routing

# ASA – všeobecné typy NAT

- Cisco ASA podporuje tieto typy NAT
  - Dynamic NAT
    - many-to-many => preklad súkromných IP adries z jedného rozsahu na verejné IP adresy z druhého poolu
  - Dynamic PAT
    - many-to-one => taktiež nazývané ako preťaženie NAT.
    - Preklad viacerých súkromných IP adries z jedného poolu preťažením vonkajšieho rozhrania alebo IP adresy
  - Static NAT
    - one-to-one => zvyčajne sa mapuje vonkajšia adresa na interný server
  - Policy NAT
    - Policy-based NAT => založené na súbore pravidiel.
    - Pravidlá určujú, že sa preložia iba určité zdrojové adresy určené pre konkrétne cieľové adresy a / alebo konkrétne porty.
- Ďalšie funkcie ASA NAT
  - Twice-NAT
    - Identifikuje zdrojovú aj cieľovú adresu v jednom pravidle (príkaz ***nat***)
    - Používa sa pri konfigurácií vzdialeného prístupu IPsec a SSL VPN

# NAT príklad

- Inside: 192.168.1.0/27
- Outside pool: 209.165.200.240 to 209.165.200.248



# ASA - konfigurácia Dynamic NAT

- Na konfiguráciu dynamického NAT sú potrebné dva sieťové objekty
  - Prvý sieťový objekt:
    - **identifikuje skupinu verejných IP adries, na ktoré sa prekladajú súkromné adresy.**
      - pomocou object príkazov ***range*** alebo ***subnet***
  - Druhý sieťový objekt
    - **identifikuje interné privátne adresy**
- Tieto dva sieťové objekty sa spoja pomocou príkazu

```
nat (real-ifc, mapped-ifc) dynamic mapped-obj.
```

```
object network PUBLIC
      range 209.165.200.240 to 209.165.200.248
object network DYNAMIC-NAT
      subnet 192.168.1.0 255.255.255.224

nat (inside, outside) dynamic PUBLIC
```

# Povolenie ICMP

- Povolenie ICMP
  - Aby neboli filtrované odpovede

```
Policy-map global_policy
     class inspection_default
     access-list ICMPACL extended permit icmp any any

Access-group ICMPACL in interface outside
```

# Overenie - *show xlate, show nat*

```
CCNAS-ASA(config)# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

NAT from inside:192.168.1.3 to outside:209.165.200.242 flags i idle 0:00:02 timeout 3:00:00
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248
CCNAS-ASA(config)#
```

# ASA - Konfigurácia Dynamic PAT

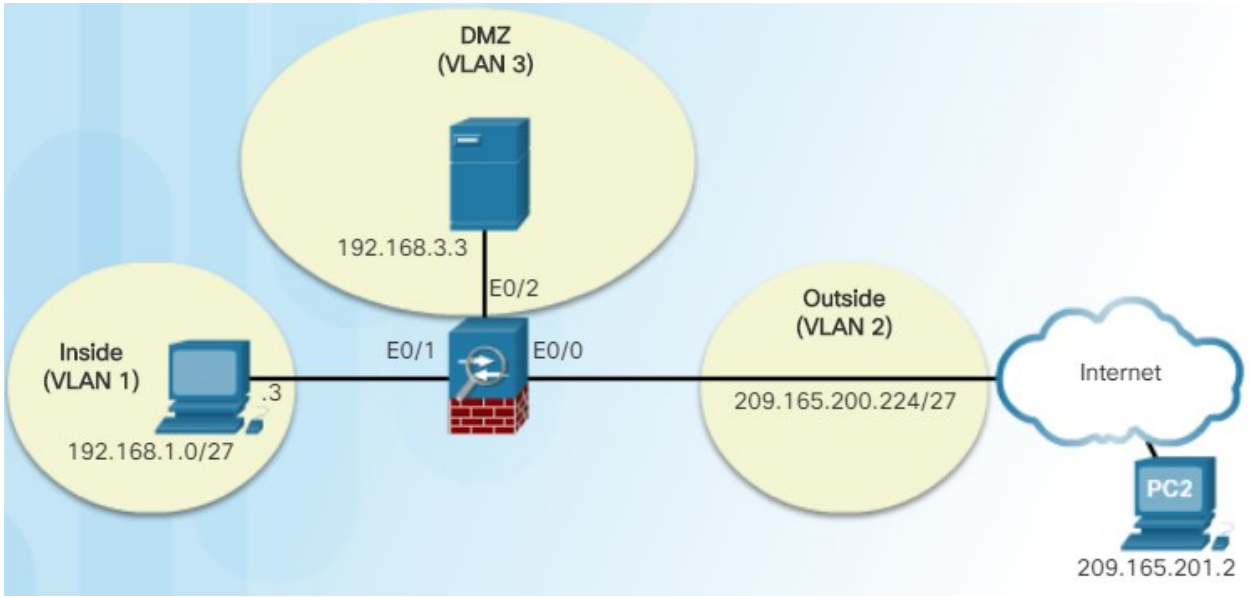
- Pri preťažení vonkajšieho rozhrania (PAT) sa vyžaduje iba jeden sieťový objekt.
- Povolenie interným hostom preťažiť vonkajšie rozhranie sa zabezpečí príkazom - ***nat*** *(real-ifc,mapped-ifc)* ***dynamic interface***

```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

```
CCNAS-ASA# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.3/1 to outside:209.165.200.226/1 flags ri idle
 0:00:02 timeout 0:00:30
CCNAS-ASA#
```

# ASA - Konfigurácia Statického NAT

- napr. ak je potrebné aby server bol prístupný aj z vonku
- Konfiguračný príkaz
  - ***nat (****real-ifc,mapped-ifc****) static*** *mapped-inline-host-ip*




```
CCNAS-ASA(config)# interface Vlan3
CCNAS-ASA(config-if)# no forward interface Vlan1
CCNAS-ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

```
CCNAS-ASA(config)# object network DMZ-SERVER
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)#  class inspection_default
CCNAS-ASA(config-pmap-c)#  access-list ICMPACL extended permit icmp any any
CCNAS-ASA(config)# access-group ICMPACL in interface dmz
CCNAS-ASA(config)#
```

```
CCNAS-ASA(config)# show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.2.3 to outside:209.165.200.227
    flags s idle 0:00:21 timeout 0:00:00

NAT from inside:192.168.1.3 to outside:209.165.200.242 flags i idle 0:09:06 timeout
 3:00:00
CCNAS-ASA(config)#
CCNAS-ASA(config)# show nat detail

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ-SERVER 209.165.200.227
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.2.3/32, Translated: 209.165.200.227/32
2 (inside) to (outside) source dynamic DYNAMIC-NAT PUBLIC
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248
CCNAS-ASA(config)#
```


# AAA

AAA

Lokálna databáza a server

Konfigurácia AAA

# AAA

- Autentifikácia, autorizácia a účtovanie poskytujú ďalšiu úroveň ochrany.
- Iba pomocou AAA sa môžu autentifikovaný a autorizovaný používatelia pripájať cez ASA.
- Autentifikácia riadi prístup vyžadovaním platných používateľských poverení, ktorými sú zvyčajne meno a heslo.
  - ASA môže autentifikovať všetky pripojenia k ASA vrátane
    - Telnet, SSH, konzoly, ASDM pomocou HTTPS a privilegovaného EXEC módu
- Autorizácia riadi prístup užívateľa po jeho autentifikácií.
  - môže autorizovať príkazy na správu, prístup do siete a prístup VPN
- Účtovanie
  - sleduje prenos, ktorý prechádza cez ASA
  - umožňuje správcom mať záznam o činnosti používateľa
  - zahŕňa čas začiatku a konca relácie užívateľa, užívateľské mená, počet bajtov ktoré precádzajú cez ASA atď...

# Lokálna databáza a server

- Cisco ASA
  - Autentifikácia pomocou lokálnej databázy (mená a heslá sú uložené lokálne na ASA)
    - ***username*** *name* ***password*** *password* ***[privilege*** *priv-level]*
    - ***clear config username*** *[name]*
    - ***show running-config username***
  - Autentifikácia pomocou externého servera (Radius alebo TACACS+)

| ASA Command | Description |
|---|---|
| `aaa-server server-tag protocol protocol` | • Creates a TACACS+ or RADIUS AAA server group. |
| `aaa-server server-tag [(interface-name)] host {server-ip \| name} [ key ]` | • Configures a AAA server as part of a AAA server group.<br>• Also configures AAA server parameters that are host-specific. |

# Konfigurácia TACACS + na ASA 5505

- Na autentifikáciu používateľov, ktorý pristupujú k ASA CLI cez konzolu, SSH, Telnet atď... použijeme príkaz:
  - ***aaa authentication*** *{* ***serial*** | ***enable*** | ***telnet*** | ***ssh*** | ***http*** *}* ***console*** *{* ***LOCAL*** | *server-group [* ***LOCAL*** *]}*
  - ***clear config aaa***

```
CCNAS-ASA(config)# username Admin password class privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run username
username Admin password obYXcKAuUW.jT5NE encrypted privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa-server TACACS-SVR protocol tacacs+
CCNAS-ASA(config-aaa-server-group)# aaa-server TACACS-SVR (dmz) host 192.168.2.3
CCNAS-ASA(config-aaa-server-host)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run aaa-server
aaa-server TACACS-SVR protocol tacacs+
aaa-server TACACS-SVR (dmz) host 192.168.2.3
 key *****
CCNAS-ASA(config)#
```

```
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication enable console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication serial console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication ssh console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run aaa
aaa authentication enable console TACACS-SVR LOCAL
aaa authentication http console TACACS-SVR LOCAL
aaa authentication serial console TACACS-SVR LOCAL
aaa authentication ssh console TACACS-SVR LOCAL
aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)# exit
CCNAS-ASA# disable
CCNAS-ASA> exit

Logoff

Username: Admin
Password: *****
Type help or '?' for a list of available commands.
CCNAS-ASA>
```

# Modular Policy Framework (MPF)

Konfigurácia class maps

Definovanie a aktivácia politiky

Prednastavené ASA politiky

# Čo je MPF?

- Definuje súbor pravidiel na uplatňovanie funkcií brány firewall
  - kontrola prevádzky a QoS, na prenos cez ASA
- Umožňuje podrobnú klasifikáciu jednotlivých tokov prevádzky, na aplikovanie rôznych pokročilých politík na jednotlivé toky.
  - MPF sa využíva s hardvérovými modulmi na presnejšie smerovanie z ASA na zariadenia využívajúce Cisco MPF.
  - Keďže podporuje kontrolu 5 až 7 vrstvy, je možné využiť ASA MPF na priradenie HTTP URL na zabránenie používateľom surfovať na konkrétnych webových stránkach v konkrétnych časoch, alebo sťahovať súbory (napr. Mp3 cez HTTP/FTP alebo HTTPS/SFTP).
- MPF využíva tri konfiguračné objekty na definovanie politík:
  - **Classify Traffic** (klasifikácia prevádzky pomocou *class mapy*)
  - **Define Actions** (definovanie akcií pomocou *policy mapy*)
  - **Activate policy** (aktivovanie politiky pomocou *service policy*)
- 4 kroky konfigurácie
  - 1. (voliteľné) konfigurácia rozšírených ACLs na identifikáciu podrobnej prevádzky
  - 2. vytvorenie class mapy, na identifikovanie prevádzky
  - 3. vytvorenie policy mapy, na aplikovanie akcií pre vytvorené class mapy
  - 4. konfigurácia service policy, na aplikovanie politiky na rozhranie

# Konfigurácia class mapy, policy mapy a aplikovanie politiky

- class mapa identifikuje prevádzku na 3-4 vrstve

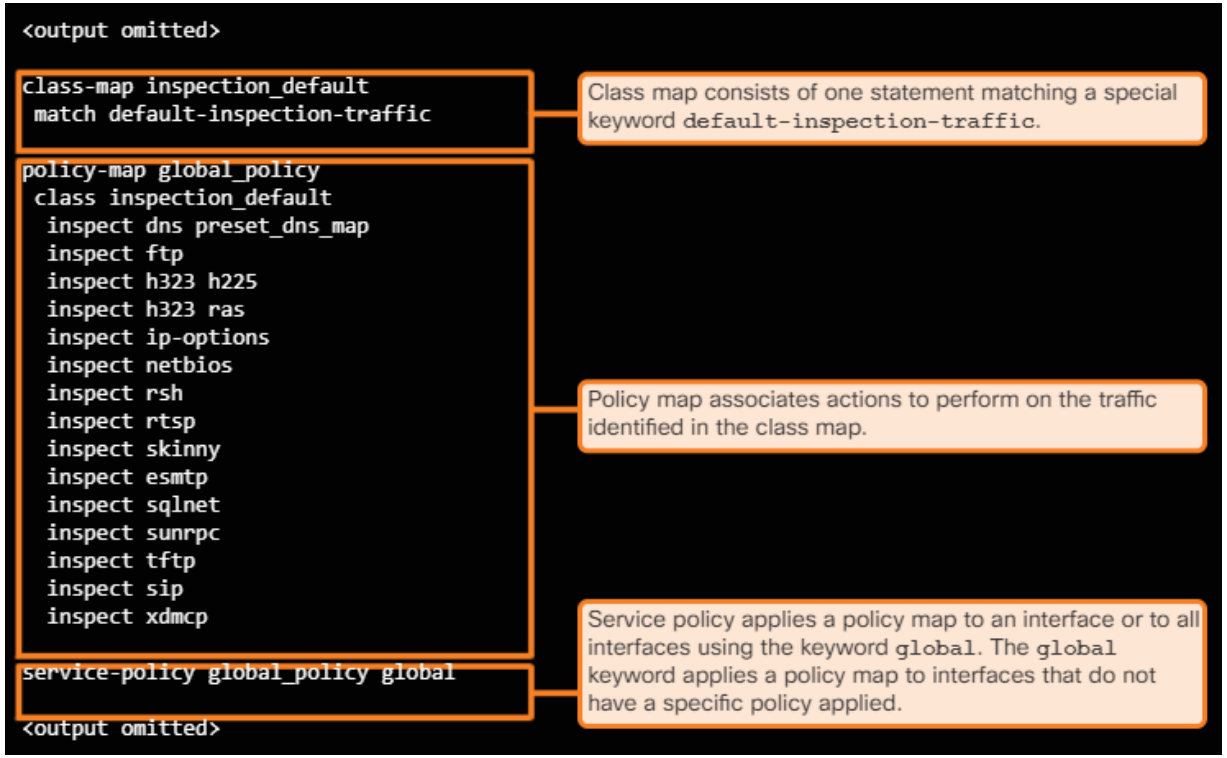
```
CCNAS-ASA(config)# access-list UDP permit udp any any
CCNAS-ASA(config)# access-list TCP permit tcp any any
CCNAS-ASA(config)# access-list SERVER permit ip any host 10.1.1.1
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-TCP
CCNAS-ASA(config-cmap)# description "This class-map matches all TCP traffic"
CCNAS-ASA(config-cmap)# match access-list TCP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-UDP
CCNAS-ASA(config-cmap)# description "This class-map matches all UDP traffic"
CCNAS-ASA(config-cmap)# match access-list UDP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-HTTP
CCNAS-ASA(config-cmap)# description "This class-map matches all HTTP traffic"
CCNAS-ASA(config-cmap)# match port TCP eq http
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map TO-SERVER
CCNAS-ASA(config-cmap)# description "Class map matches traffic  10.1.1.1"
CCNAS-ASA(config-cmap)# match access-list SERVER
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
```

Aplikovanie politiky

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

# ASA - predvolená politika

- ASA obsahuje predvolenú globálnu politiku
  - zhoduje sa so všetkým základným aplikačným prenosom
  - využíva kontrolu prenosu globálne
- Politiky aplikované na rozhranie majú prednosť pred globálnymi politikami.
- Zmena globálnej politiky
  - upraviť predvolenú politiku
  - deaktivovať predvolenú politiku
- Príkazy
  - ***show service-policy***
  - ***show running-config service-policy***
  - ***clear configure service-policy***
  - ***clear service-policy***



UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics



MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

# Ďakujem za pozornosť

Netacad kapitola 9

Implementing the Cisco Adaptive Security Appliance (ASA)