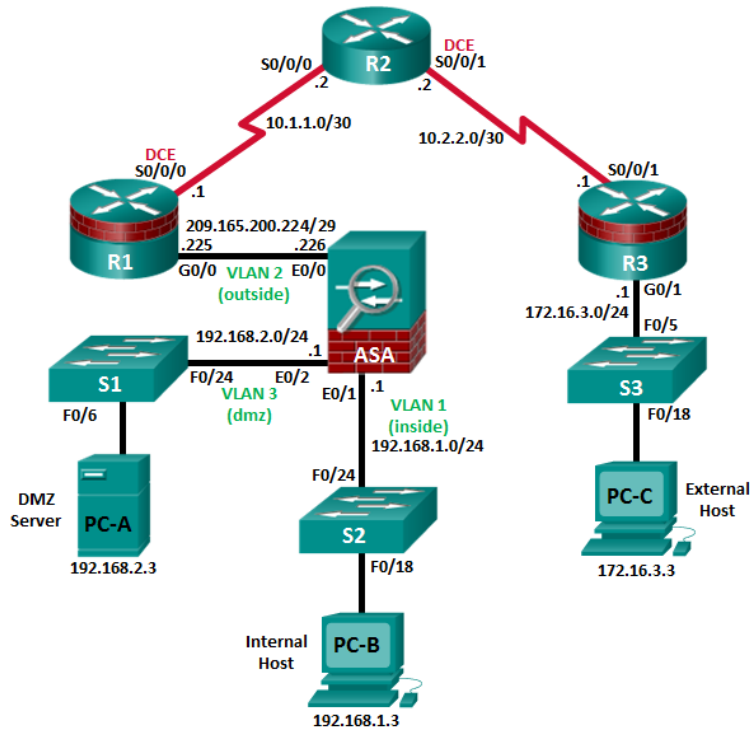


Cvičení: Konfigurace firewallu ASA 5505



Tabulka IP adres

Zařízení	Rozhraní	IP Adresy	Maska podsítě	Defaultní brána (gateway)	Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA	S2 F0/24
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA	R1 G0/0
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Celková výchozí situace

- Topologie ustanovena.
- Síť je propojena tak, jak je uvedeno v topologii.
- Jsou nakonfigurovány názvy PC a adresy IP rozhraní pro směrovače, přepínače a počítače.
- Je nakonfigurováno statického směrování, včetně výchozích tras, mezi R1, R2 a R3.
- Je povolen přístup SSH pro R1.
- Jsou nastaveny IP adresy na PC.
- Je ověřené propojení mezi PC, přepínači a směrovači.
- Je uložena základní konfigurace na směrovači.

Scénář

Zařízení Cisco Adaptive Security Appliance (ASA) je pokročilé zařízení pro zabezpečení sítě, které integruje stavovou firewall, VPN a další funkce. V rámci tohoto cvičení je zařízení ASA 5505 použito k vytvoření firewallu a ochraně interní podnikové sítě před útoky z Internetu, přičemž interním hostitelům umožňuje přístup k Internetu.

ASA vytváří tři bezpečnostní rozhraní: Outside, Inside a DMZ. Poskytuje externím uživatelům omezený přístup k DMZ a žádný přístup k vnitřním zdrojům. Vnitřní uživatelé mají přístup k DMZ a externím zdrojům.

Zaměřením tohoto cvičení je konfigurace ASA jako základního firewallu. Ostatní zařízení budou mít minimální konfiguraci, a to tak, aby podporovala ASA. Tato laboratoř používá rozhraní ASA CLI, které je podobné službě IOS CLI, pro konfiguraci základního nastavení zařízení a zabezpečení (je i grafické rozhraní ASDM).

Výchozím stavem cvičení je, že zařízení jiná než ASA byla nakonfigurována předem. V rámci cvičení bude provedeno základní nastavení ASA a filtry firewallu mezi vnitřními a vnějšími sítěmi. Poté bude ASA nakonfigurována pro další služby, jako jsou DHCP, AAA a SSH. V závěru cvičení nakonfigurujete DMZ na ASA a poskytnete přístup k serveru v DMZ.

Vaše společnost má jedno místo připojené k poskytovateli internetových služeb. Směrovač R1 představuje zařízení CPE (Customer Premises Equipment – zařízení, přes které se firma připojuje k zařízení poskytovatele) řízené ISP (Internet Service Provider). R2 představuje směrovač, který zprostředkovává spojení s ISP. R3 je zařízení poskytovatele připojené do Internetu, který spojí administrátora ze sítě, která byla najata k vzdálené správě Vaší sítě. ASA je bezpečnostní zařízení na okraji, které propojuje interní podnikovou síť a DMZ s ISP při poskytování NAT a DHCP služeb vnitřním hostitelům. ASA bude nakonfigurována pro správu administrátorem v interní síti a vzdáleným administrátorem. VLAN rozhraní vrstvy 3 poskytuje přístup ke třem oblastem vytvořeným v laboratoři: uvnitř, ven a DMZ. ISP přidělil veřejný prostor IP adresy 209.165.200.224/29, který bude použit pro překlad adres na ASA.

ASA 5505 se běžně používá jako bezpečnostní zařízení na okraji, které pro přístup na internet spojuje malý podnik s ISP zařízením, jako je DSL nebo kabelový modem. Defaultní (výchozí) nastavení výrobce pro ASA 5505 je následující:

- Je nakonfigurováno vnitřní rozhraní VLAN 1, které obsahuje porty přepínačů Ethernet 0/1 až 0/7. Adresa IP a maska VLAN 1 jsou 192.168.1.1 a 255.255.255.0.
- Je nakonfigurováno vnější rozhraní VLAN 2, které obsahuje port přepínače Ethernet 0/0. VLAN 2 získává svou IP adresu od poskytovatele služeb Internetu pomocí protokolu DHCP ve výchozím nastavení.
- Výchozí trasa je odvozena z výchozí brány DHCP.

- Všechny vnitřní adresy IP jsou překládány při přístupu do vnějšího prostředí pomocí rozhraní PAT (Port Address Translation – umožňuje překládat více vnitřních adres na jednu vnější) na rozhraní VLAN 2.
- Ve defaultním nastavení mohou uživatelé zevnitř sítě přistupovat vně dle ACL a externím uživatelům není umožněno přistupovat dovnitř podnikové sítě.
- Na zabezpečovacím zařízení je spuštěn server DHCP, takže počítač připojující k rozhraní VLAN 1 přijímá adresy mezi 192.168.1.5 a 192.168.1.36 (základní licence), i když se skutečný rozsah může lišit.
- HTTP server je nastaven pro ASDM a je přístupný uživatelům v síti 192.168.1.0/24.
- Není vyžadována žádná konzola ani hesla pro povolení a defaultní hostname je ciscoasa (stačí se kouknout příkazem `show running-config`).
- Ve defaultním nastavení platí politika ASA, při které je povolen provoz z rozhraní s vyšší úrovní zabezpečení na úroveň s nižší úrovní zabezpečení a je zakázán provoz z rozhraní s nižší úrovní zabezpečení na úroveň s vyšší úrovní zabezpečení. Defaultní nastavení ASA umožňují odchozí provoz, který je kontrolován. Zpětný provoz je povoleno kvůli kontrole na firewallu typu Stateful Packet Inspection (kontroluje se správnost posloupnosti kroků protokolů). Toto defaultní chování firewallu ASA umožňuje, aby pakety byly směrovány z vnitřní sítě do vnější sítě, nikoliv však naopak. V další části tohoto cvičení si nakonfigurujete NAT ke zvýšení ochrany firewallu.

Jednotlivé kroky nastavení

- Úvodní nastavení na ASA
- Nastavení hodnot pro vlan 1 a vlan 2
- Přiřazení portu e0/1 na vlan 1, portu e0/0 na vlan 2
- Kontrola nastavení
- Nastavení statické trasy směrovačů na ASA
- Nastavení NAT
- Nastavení politiky
- Nastavení DHCP na ASA
- Nastavení AAA autentizace a SSH
- Připojení pomocí SSH klíčů na ASA
- Konfigurace na ASA rozhraní do VLAN 3, tj. na DMZ
- Konfigurace statické NAT na DMZ
- Konfigurace statické NAT na DMZ server s použitím síťových objektů
- Konfigurace ACL přístupu na DMZ server pro uživatele z internetu
- Test přístupu na DMZ server pro externí a interní uživatele

Výchozí konfigurace firewallu

```
ciscoasa#sh run
```

```
ASA Version 8.4(2)
```

```
!
```

```
hostname ciscoasa
```

```
!
```

```
interface Ethernet0/0
```

```
switchport access vlan 2
```

```
!
```

```
interface Ethernet0/1
```

```
!
```

```
interface Ethernet0/2
```

```
!
```

```
interface Ethernet0/3
```

```
!
```

```
interface Ethernet0/4
```

```
!
```

```
interface Ethernet0/5
```

```
!
```

```
interface Ethernet0/6
```

```
!
```

```
interface Ethernet0/7
```

```
!
```

```
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
```

```
!
```

```
telnet timeout 5
```

```
ssh timeout 5
```

```
!
```

```
dhcpd auto_config outside
```

```
!
```

```
dhcpd address 192.168.1.5-192.168.1.36 inside
```

Kroky nastavení konfigurace ASA na Packet Traceru 7.1

Úvodní nastavení

```
Ciscoasa> enable
Password: <enter>
Ciscoasa#: configure terminal
Ciscoasa(config)#: hostname CCNAS-ASA
CCNAS-ASA(config)#: domain-name ccnasecurity.com
CCNAS-ASA(config)#: enable password ciscoenpa55
```

Nastavení hodnot pro vlan 1 a vlan 2

```
CCNAS-ASA(config)#int vlan 1
CCNAS-ASA(config-if)#nameif inside
CCNAS-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#security-level 100
CCNAS-ASA(config)#int vlan 2
CCNAS-ASA(config-if)#nameif outside
CCNAS-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)#security-level 0
CCNAS-ASA(config-if)#exit
```

Přiřazení port e0/1 na vlan 1, port e0/0 na vlan 2

```
CCNAS-ASA(config)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shutdown
```

Kontrola

```
CCNAS-ASA#show int ip brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 unassigned YES unset up up
Ethernet0/1 unassigned YES unset up up
Ethernet0/2 unassigned YES unset up up
Ethernet0/3 unassigned YES unset down down
Ethernet0/4 unassigned YES unset down down
Ethernet0/5 unassigned YES unset down down
Ethernet0/6 unassigned YES unset down down
Ethernet0/7 unassigned YES unset down down
Vlan1 192.168.1.1 YES manual up up
Vlan2 209.165.200.226 YES manual up up
```

Kontrola - PC-B --- ping na ASA

```
C:\>ping 192.168.1.1
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
C:\>ping 209.165.200.225
Request timed out.
Request timed out.
Request timed out.
```

Nastavení statické trasy směrovačů na ASA

```
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225  
Pingnout z ASA na R1 s0/0/0 (pingnutí musí být úspěšné)
```

Nastavení NAT

```
CCNAS-ASA(config)#object network inside-net  
CCNAS-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0  
CCNAS-ASA(config-network-object)#nat (inside,outside) dynamic interface  
CCNAS-ASA(config-network-object)#exit  
Ověření NAT příkazem show run object
```

Nastavení politiky

```
CCNAS-ASA(config)#class-map inspection_default  
CCNAS-ASA(config-cmap)#match default-inspection-traffic  
CCNAS-ASA(config-cmap)#exit  
CCNAS-ASA(config)#policy-map global_policy  
CCNAS-ASA(config-pmap)#class inspection_default  
CCNAS-ASA(config-pmap-c)#inspect icmp  
CCNAS-ASA(config-pmap-c)#exit  
CCNAS-ASA(config)#service-policy global_policy global
```

Kontrola – PC-B

```
C:\>ping 209.165.200.225  
    Reply from 209.165.200.225: bytes=32 time=14ms TTL=254  
    Reply from 209.165.200.225: bytes=32 time<1ms TTL=254  
    Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
```

Nastavení DHCP na ASA

```
CCNAS-ASA(config)#dhcp address 192.168.1.5-192.168.1.36 inside  
CCNAS-ASA(config)#dhcp dns 209.165.201.2 interface inside  
CCNAS-ASA(config)#dhcp enable imide
```

PC-B – přepnout se static IP na DHCP ip konfiguraci

Nastavení AAA autentizace a SSH

```
CCNAS-ASA(config)#username admin password adminpa55  
CCNAS-ASA(config)#aaa authentication ssh console LOCAL  
CCNAS-ASA(config)#crypto key generate rsa modulus 1024  
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
```

```
Do you really want to replace them? [yes/no]: no  
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

```
CCNAS-ASA(config)#ssh 192.168.1.0 255.255.255.0 inside  
CCNAS-ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
```

Připojení pomocí SSH klíčů na ASA

```
PC-C  
C:\>ssh -l admin 209.165.200.226  
Open  
Password: adminpa55  
CCNAS-ASA>  
PC-B
```

```
C:\>ssh -l admin 192.168.1.1
Open
Password: adminpa55
CCNAS-ASA>
```

Konfigurace DMZ na rozhraní Vlan 3

```
CCNAS-ASA(config-if)# interface vlan 3
CCNAS-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)#nameif dmz
CCNAS-ASA(config-if)#no forward interface vlan 1
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)#no shut
CCNAS-ASA(config-if)#exit
```

Konfigurace statické NAT na DMZ

```
CCNAS-ASA(config)#int e0/2
CCNAS-ASA(config-if)#switchport access vlan 3
CCNAS-ASA(config-if)#no shut
```

```
CCNAS-ASA#show int ip brief
```

```
Interface IP-Address OK? Method Status Protocol
```

```
Ethernet0/0 unassigned YES unset up up
Ethernet0/1 unassigned YES unset up up
Ethernet0/2 unassigned YES unset up up
Ethernet0/3 unassigned YES unset down down
Ethernet0/4 unassigned YES unset down down
Ethernet0/5 unassigned YES unset down down
Ethernet0/6 unassigned YES unset down down
Ethernet0/7 unassigned YES unset down down
Vlan1 192.168.1.1 YES manual up up
Vlan2 209.165.200.226 YES manual up up
Vlan3 192.168.2.1 YES manual up up
```

```
CCNAS-ASA# show ip address
```

```
System IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
Vlan1	inside	192.168.1.1	255.255.255.0	manual
Vlan2	outside	209.165.200.226	255.255.255.248	manual
Vlan 3	dmz	192.168.2.1	255.255.255.0	manual

Konfigurace statické NAT na DMZ server s použitím síťových objektů

```
CCNAS-ASA# configure terminal
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
```

Konfigurace ACL povolení přístupu na DMZ server z internetu

```
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNAS-ASA(config)#access-group OUTSIDE-DMZ in interface outsider
```

Test přístupu na server v DMZ

```
R2> enable
R2# configure terminal
R2(config-if)#interface lo0
R2(config-if)#ip address 172.30.1.1 255.255.255.0
R2(config-if)# end
R2#ping 209.165.200.227 source lo0
    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
    Packet sent with a source address of 172.30.1.1
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Finální konfigurace ASA

```
ASA Version 8.4(2)
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password 57n/mTd4HwB/bqHS encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
switchport access vlan 3
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
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 209.165.200.226 255.255.255.248
!
```



```
interface Vlan3
no forward interface Vlan1
nameif dmz
security-level 70
ip address 192.168.2.1 255.255.255.0
!
object network dmz-server
host 192.168.2.3
object network inside-net
subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
access-list OUTSIDE-DMZ extended permit icmp any host 192.168.2.3
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq www
!
access-group OUTSIDE-DMZ in interface outside
object network dmz-server
nat (dmz,outside) static 209.165.200.227
object network inside-net
nat (inside,outside) dynamic interface
!
aaa authentication ssh console LOCAL
!
username admin password .vMR4ts6hGyvBErZ encrypted
!
class-map inspection_default
match default-inspection-traffic
!
policy-map global_policy
class inspection_default
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd dns 209.165.201.2 interface inside
dhcpd enable inside
!
```