Konfiguracja Cisco Zone-Based Firewall (ZBF)

1. Wprowadzenie

Zone-Based Firewall (ZBF) to nowoczesne podejście do filtrowania ruchu w routerach Cisco, zastępujące klasyczne ACL i CBAC. Bazuje na przydzieleniu interfejsów do stref (zones), a następnie definiowaniu polityk między strefami.

2. Kroki konfiguracji

2.1 Tworzenie stref

Zdefiniuj strefy, do których przypiszesz interfejsy:

```
zone security ZONA-WEW
zone security ZONA-INTERNET
```

== 2.2 Przypisanie interfejsów do stref ==

```
interface GigabitEthernet0/0
zone-member security ZONA-WEW

interface GigabitEthernet0/1
zone-member security ZONA-INTERNET
```

2.3 Tworzenie klasy ruchu

Określ, jaki typ ruchu będzie rozpoznawany:

```
class-map type inspect match-any CMAP-WWW
match protocol http
match protocol https
```

== 2.4 Tworzenie polityki ruchu ==

```
policy-map type inspect PMAP-WEW-INTERNET
class type inspect CMAP-WWW
inspect
class class-default
drop
```

== 2.5 Powiązanie polityki z ruchem między strefami ==

```
zone-pair security ZP-WEW-DO-INTERNET source ZONA-WEW destination ZONA-
```

```
INTERNET
service-policy type inspect PMAP-WEW-INTERNET
```

=== 3. Weryfikacja ===

```
show zone security
show zone-pair security
show policy-map type inspect zone-pair
```

4. Uwagi

* Jeśli interfejs nie należy do żadnej strefy, to nie może wymieniać ruchu z żadnym innym interfejsem. * Komenda `inspect` oznacza zezwolenie i śledzenie sesji. * Komenda `drop` blokuje nieokreślony ruch domyślnie.

5. Przykład rozszerzenia

Dodanie reguły dla ICMP:

```
class-map type inspect match-any CMAP-PING
match protocol icmp

policy-map type inspect PMAP-WEW-INTERNET
class type inspect CMAP-WWW
inspect
class type inspect CMAP-PING
inspect
class class-default
drop
```