Cisco ASA Firewall CLI and Its Usages

Contents

Interface Configuration

```
interface GigabitEthernet0/0
 no shutdown
 nameif SALES_VLAN
 ip address 172.16.24.1 255.255.255.0
 security-level 100
!
interface GigabitEthernet0/1
 no shutdown
 nameif OUTSIDE
 ip address 211.1.1.1 255.255.255.0
 security-level 0
!
interface GigabitEthernet0/2
 no shutdown
!
interface GigabitEthernet0/2.10
 vlan 10
 ip address 10.1.1.1 255.255.255.0
 nameif DMZ1
 security-level 50
!
interface GigabitEthernet0/2.20
 vlan 20
 ip address 20.1.1.1 255.255.255.0
 nameif DMZ2
 security-level 50
```

Time Range Configuration

```
time-range AFTERWORK
 periodic daily 17:30 to 6:00
```

Object Group Configuration

```
object-group network SALES_VLAN_TCP_SERVER
 network-object host 1.1.1.1
 network-object host 2.1.1.1
 network-object host 3.1.1.1
 network-object host 4.1.1.1
 network-object host 5.1.1.1
 network-object host 6.1.1.1
 network-object host 7.1.1.1
```


Access Control List (ACL) Configuration

```
access-list SALES_VLAN_in line 1 extended permit tcp object-group SALES_VLAN_TCP_SERVER
172.16.2.1 255.255.255.0 eq ssh time-range AFTERWORK
access-list SALES_VLAN_in line 12 extended deny tcp any any log
!
access-group SALES_VLAN_in in interface SALES_VLAN
```

High Availability (HA) Failover Configuration

```
interface GigabitEthernet0/4
 no shutdown
 failover lan unit primary
 failover lan interface FAILOVER GigabitEthernet0/4
 failover link FAILOVER GigabitEthernet0/4
 failover interface ip FAILOVER 1.1.1.1 255.255.255.0 standby 1.1.1.2
```

```
failover
!
monitor-interface OUTSIDE
monitor-interface INSIDE
monitor-interface SALES_VLAN
```

Secondary ASA HA Configuration

```
interface GigabitEthernet0/4
 no shutdown
 failover lan unit secondary
 failover lan interface FAILOVER GigabitEthernet0/4
 failover link FAILOVER GigabitEthernet0/4
 failover interface ip FAILOVER 1.1.1.1 255.255.255.0 standby 1.1.1.2
 failover
!
monitor-interface OUTSIDE
monitor-interface INSIDE
monitor-interface SALES_VLAN
```


NAT Configuration

```
object network dynamic_public_mapped_ip
 range 211.1.1.2 211.1.1.10
!
object network sales_vlan_inside
 network 172.16.24.0 255.255.255.0
 nat (SALES_VLAN,OUTSIDE) dynamic dynamic_public_mapped_ip
```

Context Creation

```
class gold
 limit-resource mac-addresses 10000
 limit-resource conns 15%
 limit-resource rate conns 1000
 limit-resource asdm 5
 limit-resource ssh 5
 limit-resource telnet 5
 limit-resource xlates 36000
!
class silver
 limit-resource mac-addresses 8000
 limit-resource conns 7%
 limit-resource rate conns 300
 limit-resource asdm 2
 limit-resource ssh 3
 limit-resource telnet 1
 limit-resource xlates 3000
!
admin-context administrator
context administrator
 allocate-interface GigabitEthernet0/0
 config-url flash:/admin.cfg
!
context c1
 allocate-interface GigabitEthernet0/1
 config-url flash:/c1.cfg
 member gold
```

```
!
context c2
 allocate-interface GigabitEthernet0/2
 config-url flash:/c2.cfg
 member silver
```

Modular Policy Framework (MPF) Configuration

```
policy-map MY-POLICY
 class inspection_default
  inspect ftp
  inspect http
```

Routing Configuration

```
router ospf 100
 network 10.0.0.0 255.0.0.0 area 0
 router-id 1.1.1.1
```


VPN Configuration

```
! Phase 1 Configuration
crypto isakmp policy 10
 encryption aes-256
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400
!
crypto isakmp enable OUTSIDE
!
! Phase 2 Configuration
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
! Tunnel Group Configuration
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
 pre-shared-key MY_SECRET_KEY
```

```
!
! Crypto Map Configuration
crypto map VPN-MAP 10 match address VPN_ACL
crypto map VPN-MAP 10 set peer 192.168.1.1
crypto map VPN-MAP 10 set transform-set VPN-SET
crypto map VPN-MAP interface OUTSIDE
!
! ACL for VPN Traffic
access-list VPN_ACL extended permit ip 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0
```

Troubleshooting Commands

1. show capture

   capture <name> <interface> <filter>

2. packet-tracer

   packet-tracer input <interface> <protocol> <src-ip> <dest-ip> <port>

3. show xlate

4. show access-list

5. show interface ip brief

6. show crypto ikev1 sa brief

7. show crypto ikev2 peer

8. show running-config