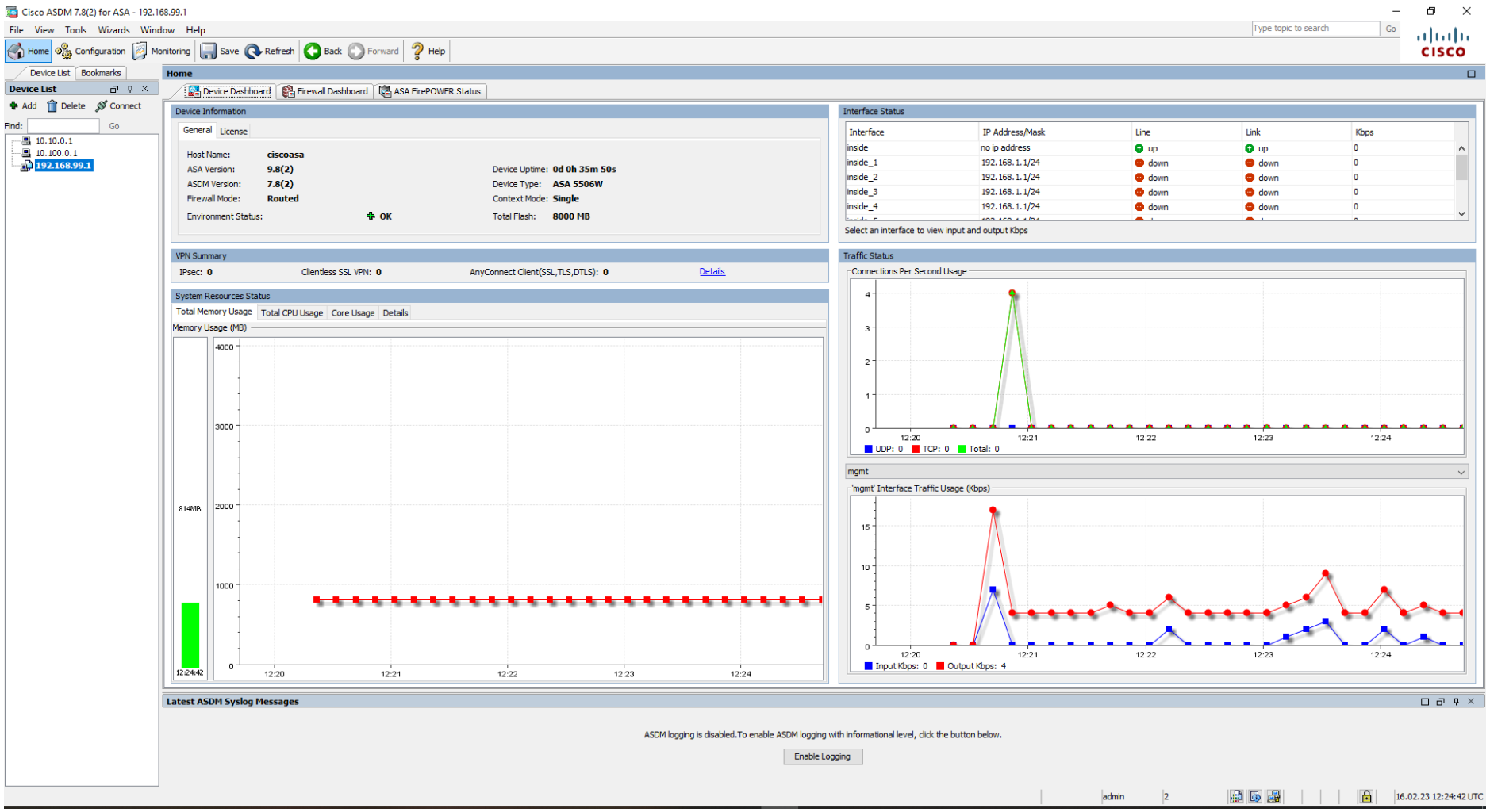
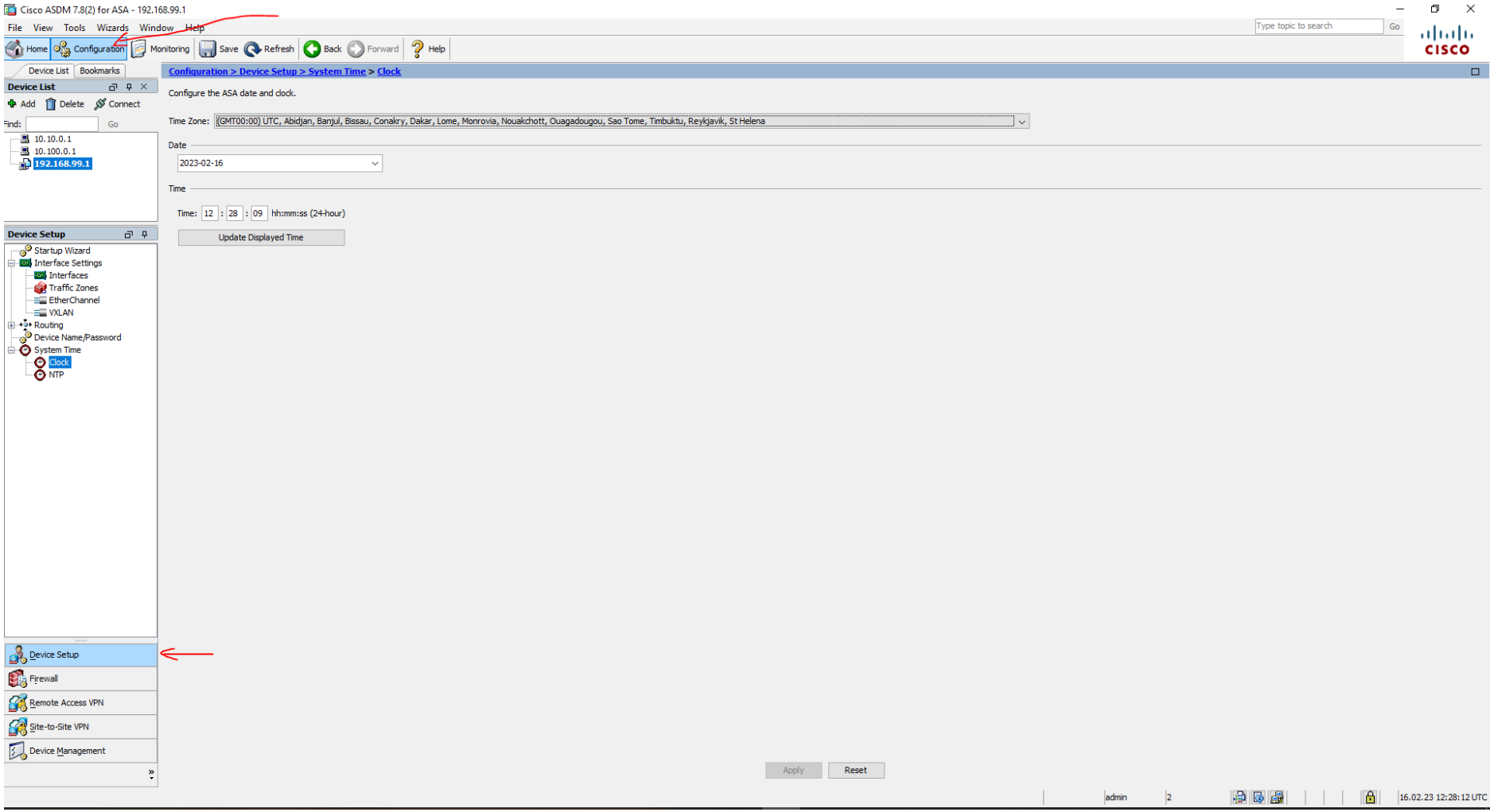
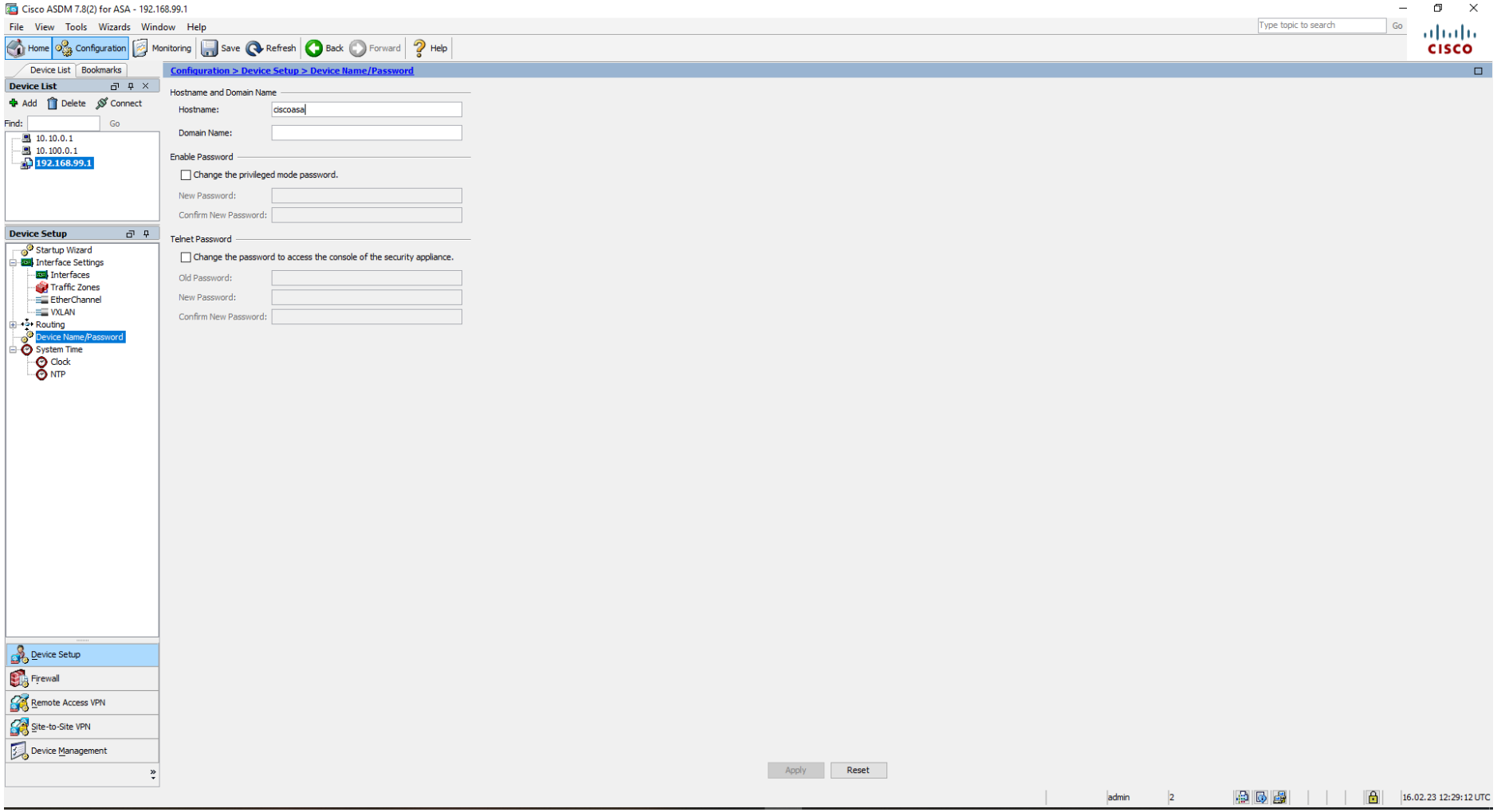
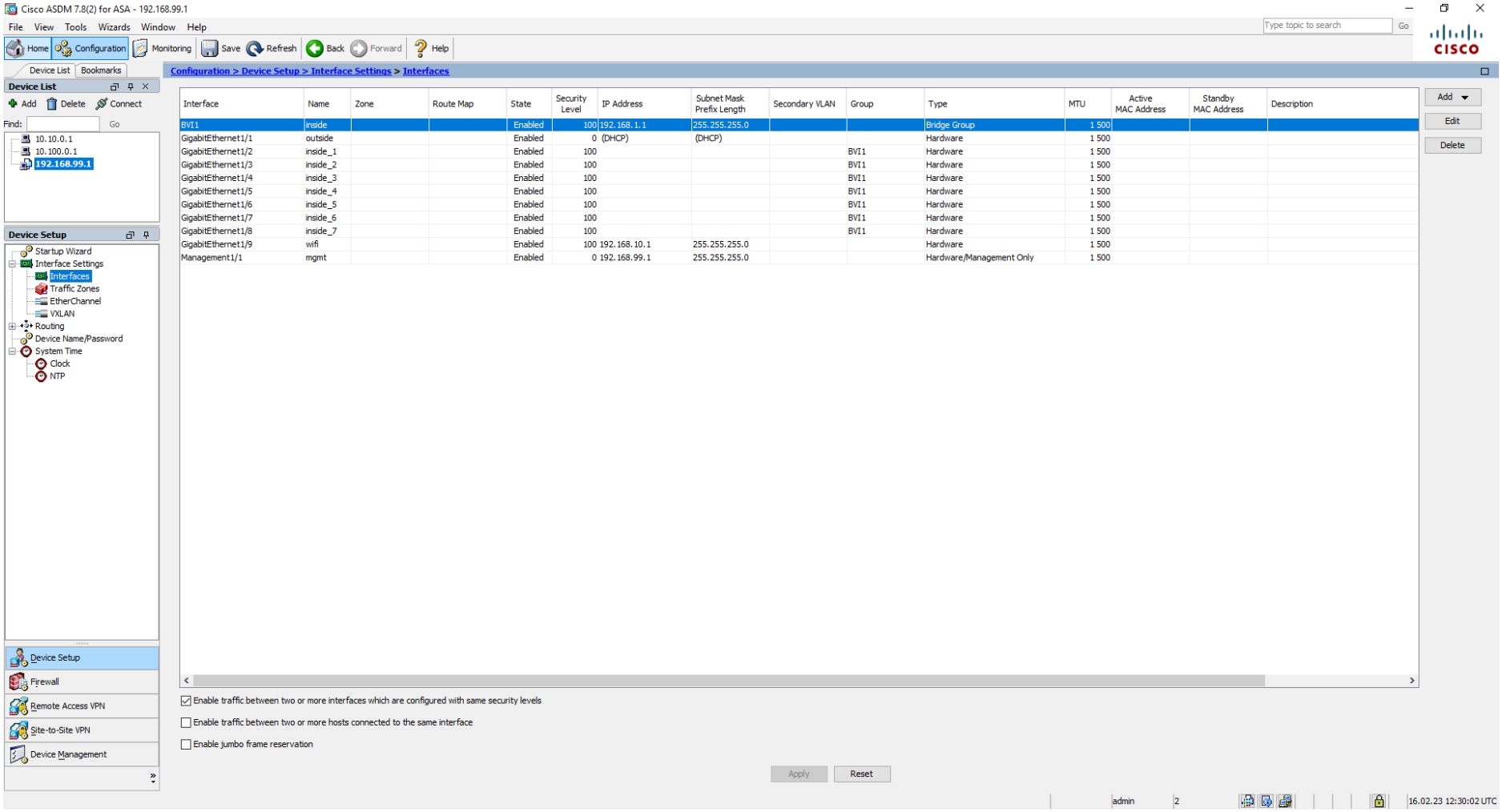
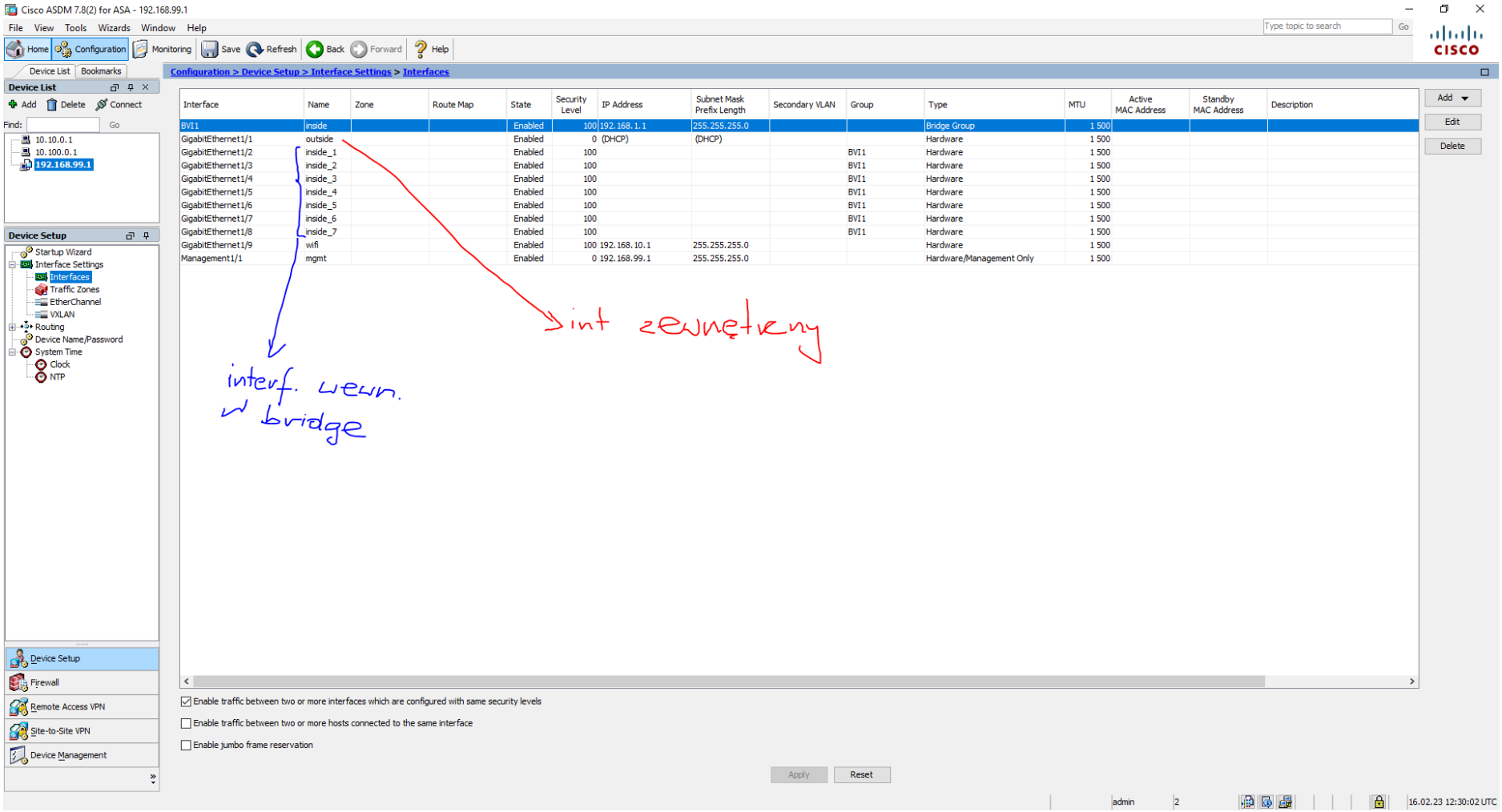
Cisco ASA 5506




Cisco ASDM 7.8(2) for ASA - 192.168.99.1
File View Tools Wizards Window Help
Type topic to search
Go
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Device List
Bookmarks
Device List
Add
Delete
Connect
Find:
Go
10.10.0.1
10.100.0.1
192.168.99.1
Device Setup
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Clock
NTP
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Setup > System Time > Clock
Configure the ASA date and clock.
Time Zone:
(GMT00:00) UTC, Abidjan, Banjul, Bissau, Conakry, Dakar, Lome, Monrovia, Nouakchott, Ouagadougou, Sao Tome, Timbuktu, Reykjavik, St Helena
Date
2023-02-16
Time
Time: 12 : 28 : 09 hh:mm:ss (24-hour)
Update Displayed Time
Apply
Reset
admin
2
16.02.23 12:28:12 UTC

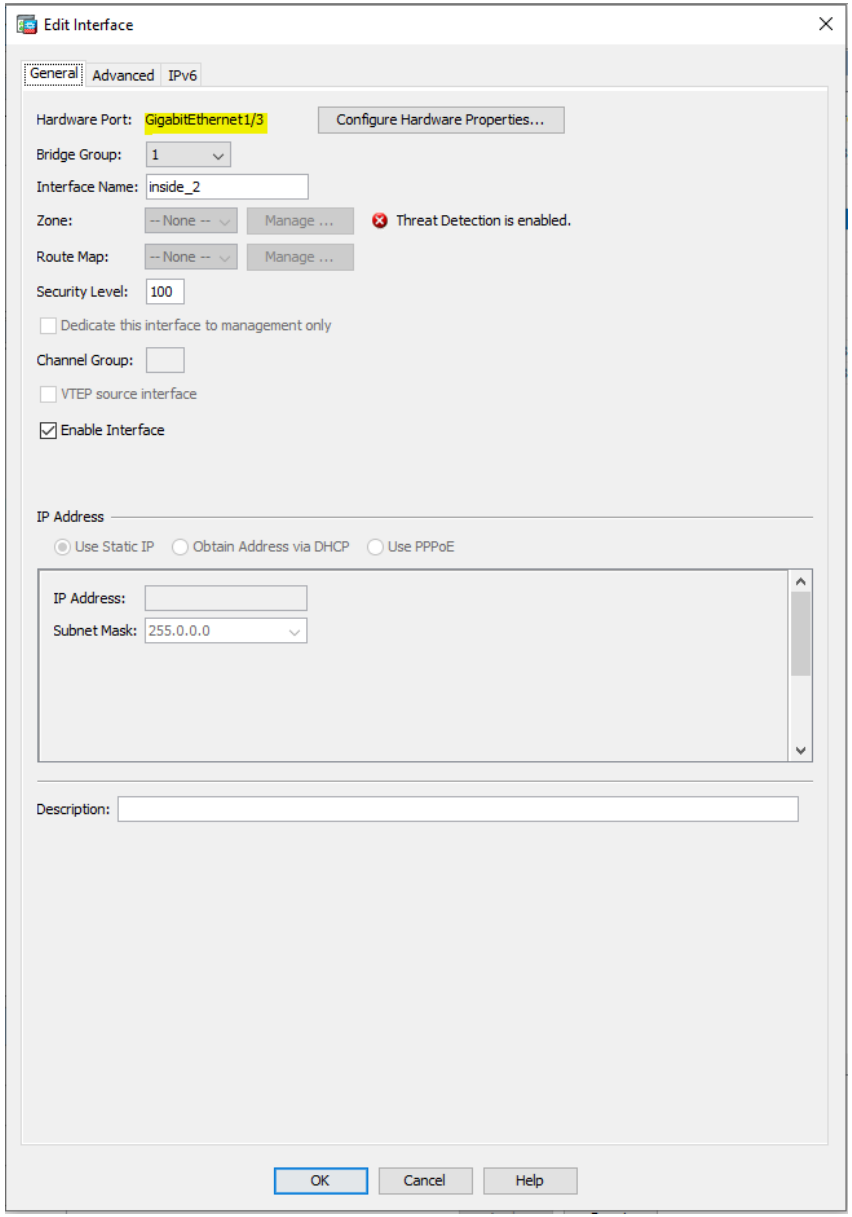

Cisco ASDM 7.8(2) for ASA - 192.168.99.1
File View Tools Wizards Window Help
Type topic to search
Go
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Device List
Bookmarks
Device List
Add
Delete
Connect
Find:
Go
10.10.0.1
10.100.0.1
192.168.99.1
Device Setup
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Clock
NTP
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Setup > Device Name/Password
Hostname and Domain Name
Hostname:
ciscoasa
Domain Name:
Enable Password
Change the privileged mode password.
New Password:
Confirm New Password:
Telnet Password
Change the password to access the console of the security appliance.
Old Password:
New Password:
Confirm New Password:
Apply
Reset
admin
2
16.02.23 12:29:12 UTC


Cisco ASDM 7.8(2) for ASA - 192.168.99.1
File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
Device List Bookmarks
Device List
Add Delete Connect
Find: Go
10.10.0.1
10.100.0.1
192.168.99.1
Device Setup
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Clock
NTP
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Setup > Interface Settings > Interfaces
Interface Name Zone Route Map State Security Level IP Address Subnet Mask Prefix Length Secondary VLAN Group Type MTU Active MAC Address Standby MAC Address Description
BVI1 inside Enabled 100 192.168.1.1 255.255.255.0 Bridge Group 1 500
GigabitEthernet1/1 outside Enabled 0 (DHCP) (DHCP) Hardware 1 500
GigabitEthernet1/2 inside_1 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/3 inside_2 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/4 inside_3 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/5 inside_4 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/6 inside_5 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/7 inside_6 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/8 inside_7 Enabled 100 BVI1 Hardware 1 500
GigabitEthernet1/9 wifi Enabled 100 192.168.10.1 255.255.255.0 Hardware 1 500
Management1/1 mgmt Enabled 0 192.168.99.1 255.255.255.0 Hardware/Management Only 1 500
Add Edit Delete
Enable traffic between two or more interfaces which are configured with same security levels
Enable traffic between two or more hosts connected to the same interface
Enable jumbo frame reservation
Apply Reset
admin 2 16.02.23 12:30:02 UTC

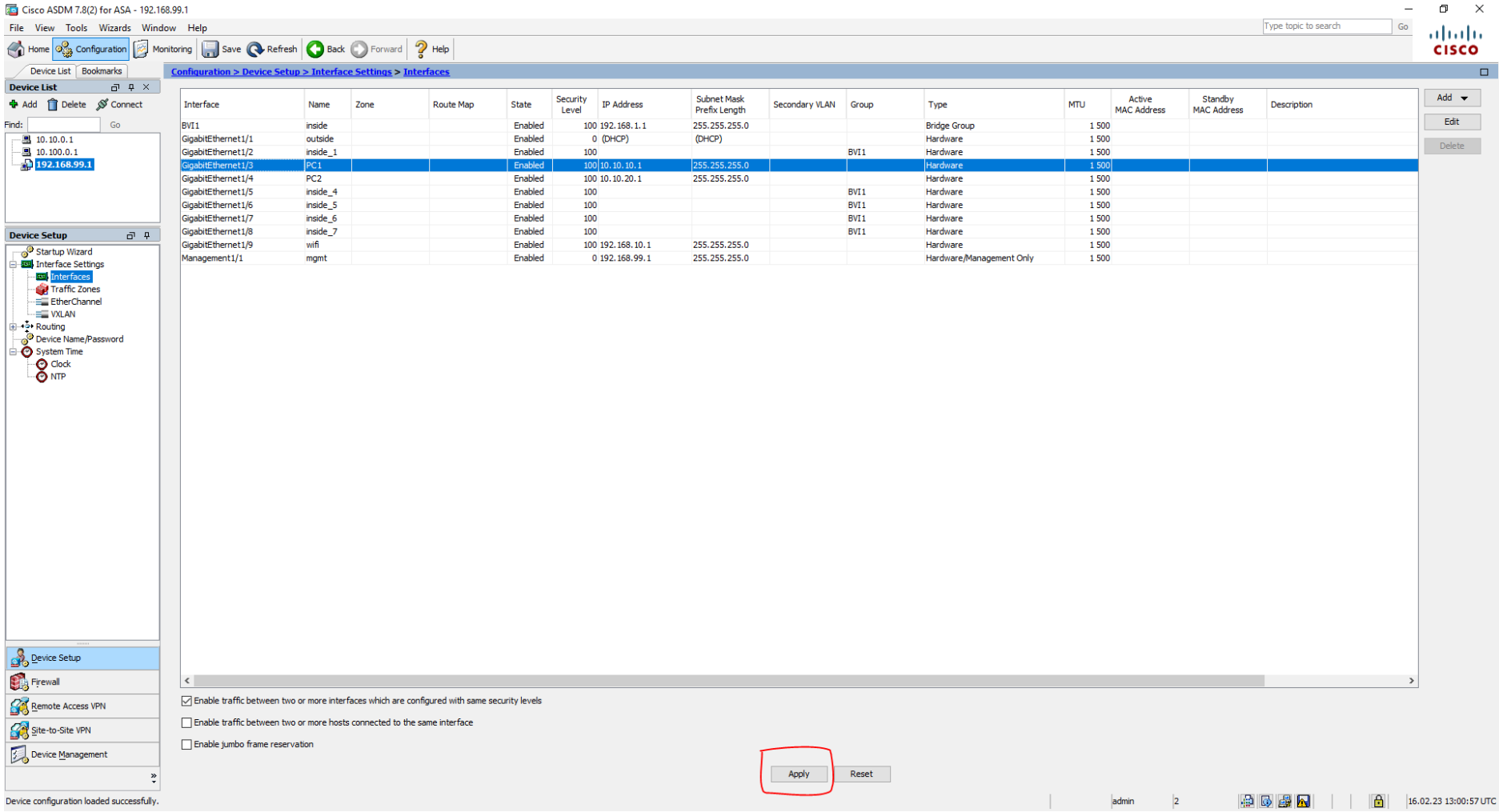


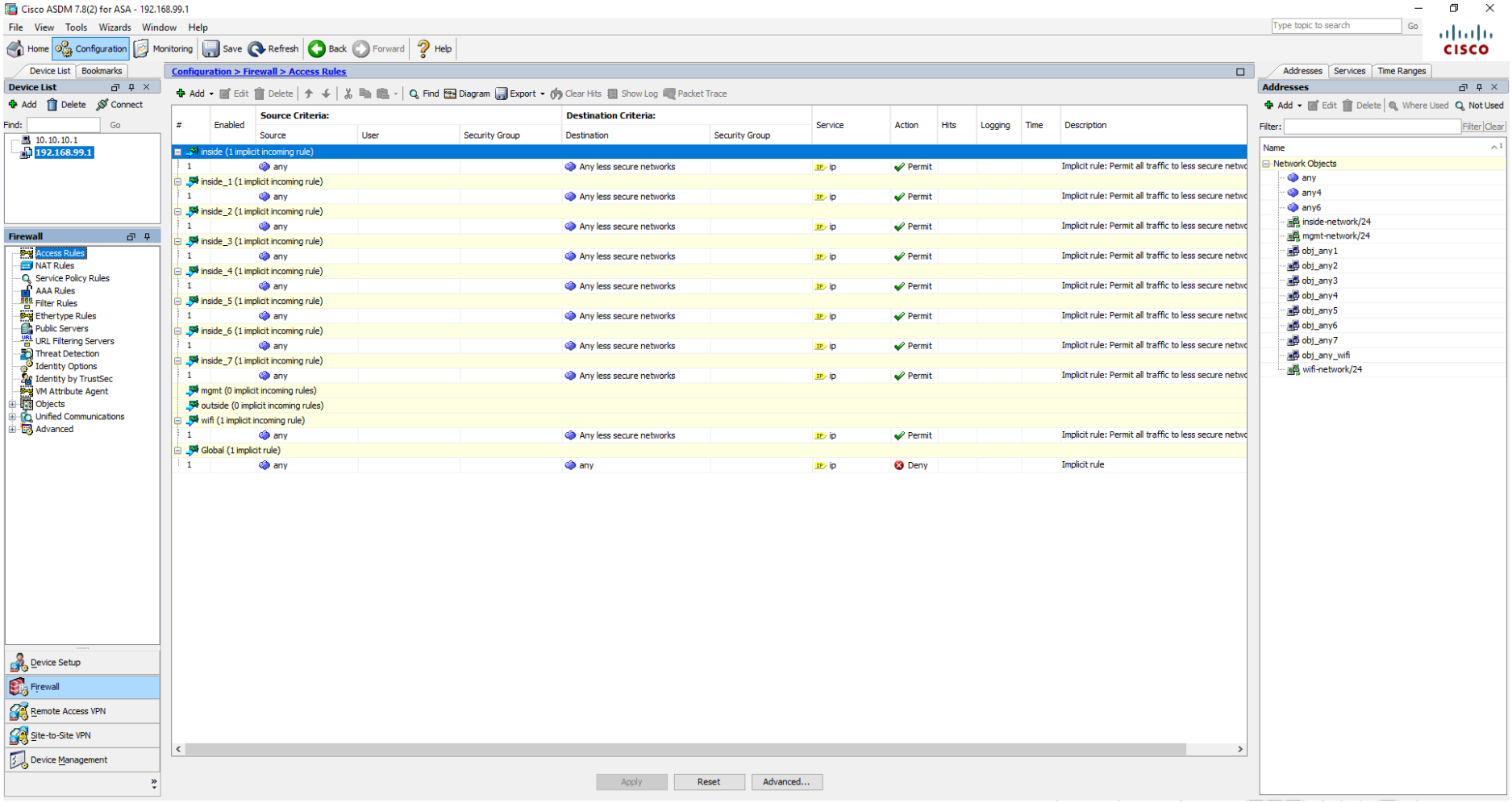
Dotyczy interfejsów inside (2-8)

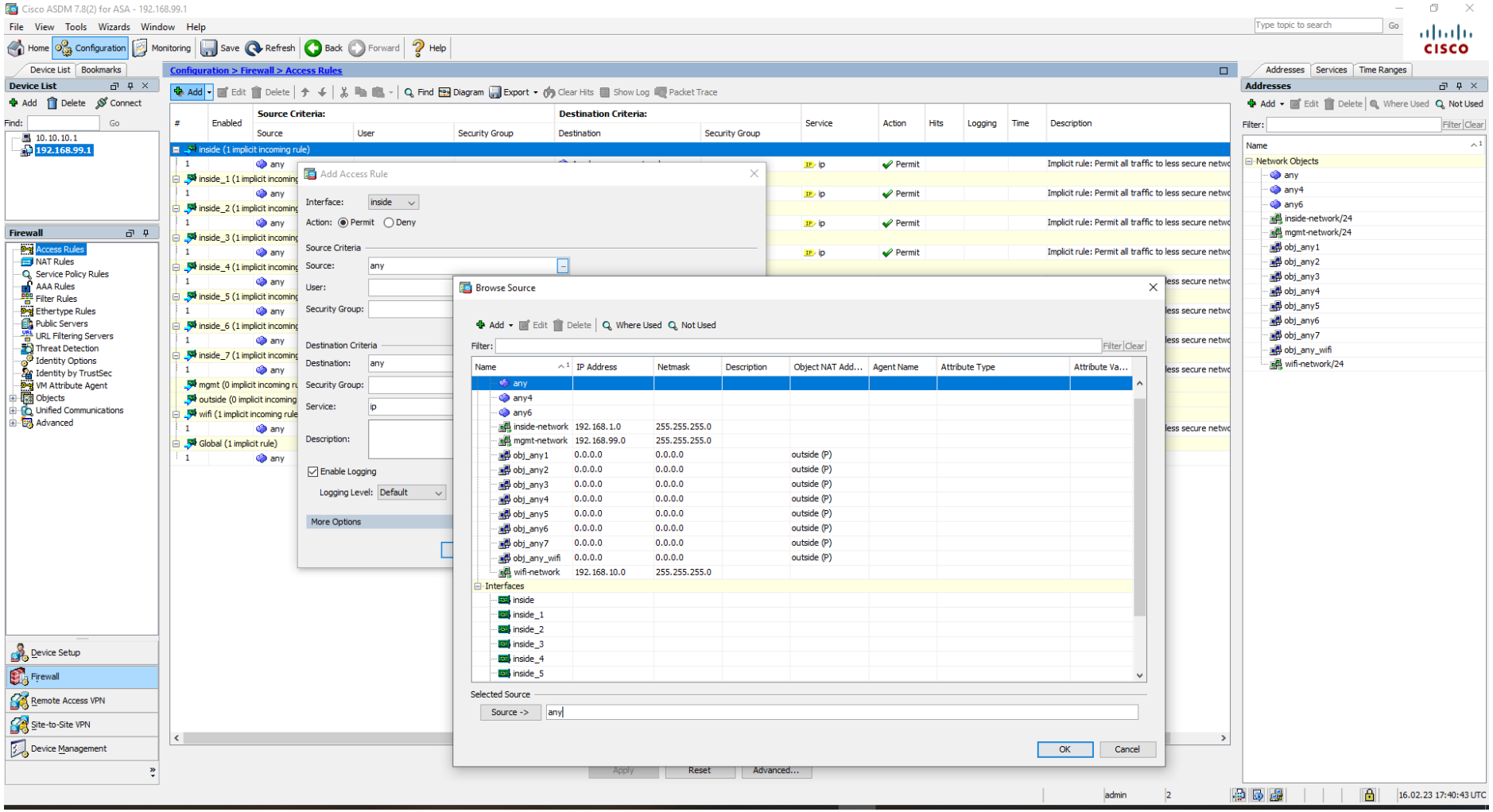
Ruch przechodzi tylko z interfejsu mającego większy security level do interfejsu z mniejszym.

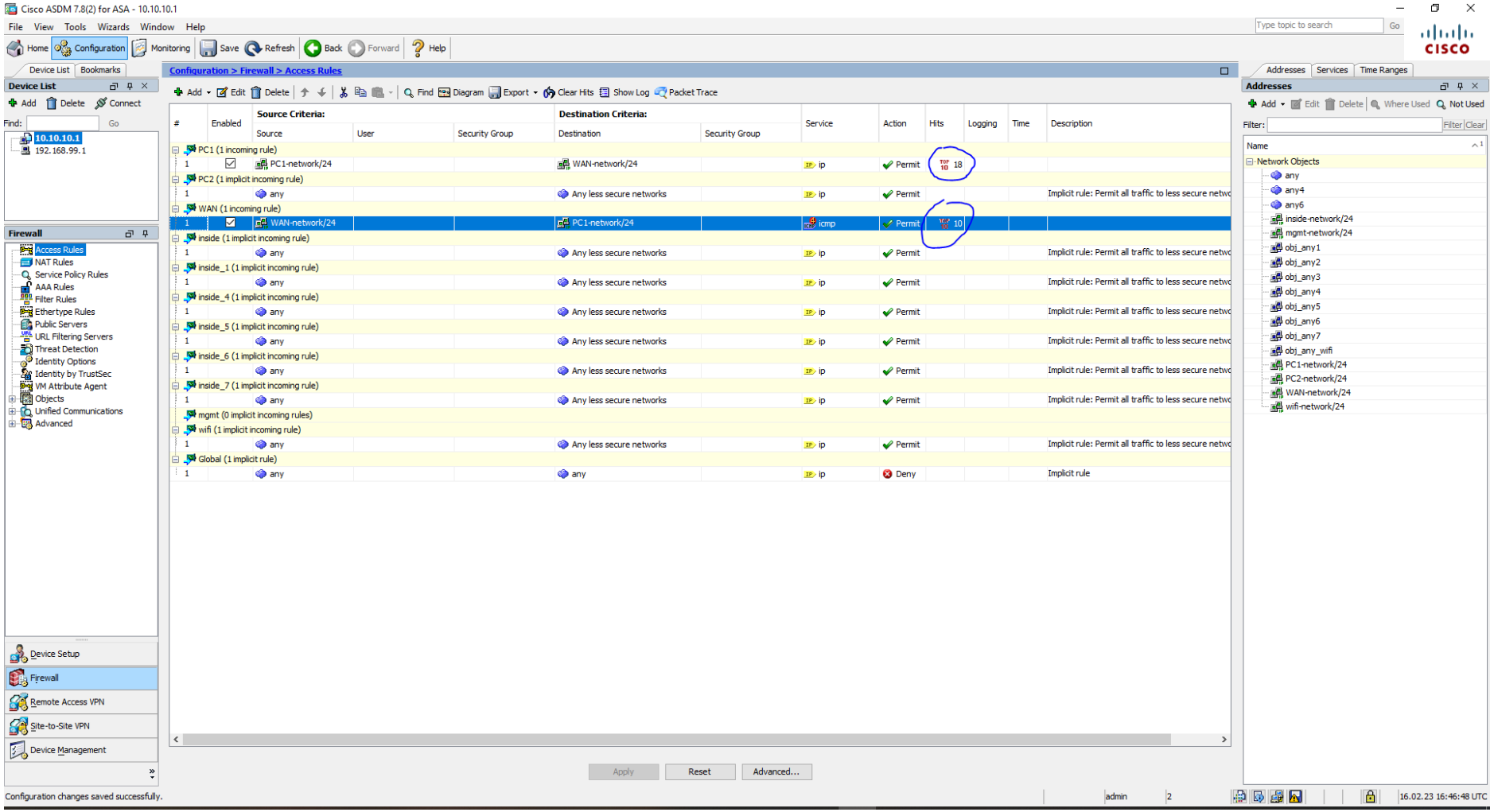

Edit Interface
General
Advanced
IPv6
Hardware Port:
GigabitEthernet1/3
Configure Hardware Properties...
Bridge Group:
1
Interface Name:
inside_2
Zone:
-- None --
Manage ...
Threat Detection is enabled.
Route Map:
-- None --
Manage ...
Security Level:
100
Dedicate this interface to management only
Channel Group:
VTEP source interface
Enable Interface
IP Address
Use Static IP
Obtain Address via DHCP
Use PPPoE
IP Address:
Subnet Mask:
255.0.0.0
Description:
OK
Cancel
Help

Zmianę w aplikacji musimy wgrać na firewalla (przycisk Apply)




Cisco ASDM 7.8(2) for ASA - 192.168.99.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List Bookmarks
Device List
Add Delete Connect
Find: Go
10.10.10.1
192.168.99.1
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Ethertype Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
VM Attribute Agent
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Enabled Source Criteria: Source User Security Group Destination Criteria: Destination Security Group Service Action Hits Logging Time Description
inside (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_1 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_2 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_3 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_4 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_5 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_6 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_7 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
mgmt (0 implicit incoming rules)
outside (0 implicit incoming rules)
wifi (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
Global (1 implicit rule)
1 any any ip Deny Implicit rule
Apply Reset Advanced...
Addresses Services Time Ranges
Addresses
Add Edit Delete Where Used Not Used
Filter: Filter Clear
Name
Network Objects
any
any4
any6
inside-network/24
mgmt-network/24
obj_any1
obj_any2
obj_any3
obj_any4
obj_any5
obj_any6
obj_any7
obj_any_wifi
wifi-network/24


Cisco ASDM 7.8(2) for ASA - 192.168.99.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Configuration > Firewall > Access Rules
Device List
Add Delete Connect
10.10.10.1
192.168.99.1
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Ethertype Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
VM Attribute Agent
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria:
Destination Criteria:
Add Access Rule
Interface: inside
Action: Permit Deny
Source Criteria
Source: any
User:
Security Group:
Destination Criteria
Destination: any
Security Group:
Service: ip
Description:
Enable Logging
Logging Level: Default
More Options
Browse Source
Add Edit Delete Where Used Not Used
Filter:
Name
IP Address
Netmask
Description
Object NAT Add...
Agent Name
Attribute Type
Attribute Va...
any
any4
any6
inside-network 192.168.1.0 255.255.255.0
mgmt-network 192.168.99.0 255.255.255.0
obj_any1 0.0.0.0 0.0.0.0 outside (P)
obj_any2 0.0.0.0 0.0.0.0 outside (P)
obj_any3 0.0.0.0 0.0.0.0 outside (P)
obj_any4 0.0.0.0 0.0.0.0 outside (P)
obj_any5 0.0.0.0 0.0.0.0 outside (P)
obj_any6 0.0.0.0 0.0.0.0 outside (P)
obj_any7 0.0.0.0 0.0.0.0 outside (P)
obj_any_wifi 0.0.0.0 0.0.0.0 outside (P)
wifi-network 192.168.10.0 255.255.255.0
Interfaces
inside
inside_1
inside_2
inside_3
inside_4
inside_5
Selected Source
Source -> any
OK Cancel
Addresses Services Time Ranges
Addresses
Add Edit Delete Where Used Not Used
Filter: Filter Clear
Name
Network Objects
any
any4
any6
inside-network/24
mgmt-network/24
obj_any1
obj_any2
obj_any3
obj_any4
obj_any5
obj_any6
obj_any7
obj_any_wifi
wifi-network/24
Apply Reset Advanced...
admin 2 16.02.23 17:40:43 UTC


Cisco ASDM 7.8(2) for ASA - 10.10.10.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria: Destination Criteria:
Enabled Source User Security Group Destination Security Group Service Action Hits Logging Time Description
PC1 (1 incoming rule)
1 PC1-network/24 WAN-network/24 ip Permit 18
PC2 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
WAN (1 incoming rule)
1 WAN-network/24 PC1-network/24 icmp Permit 10
inside (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_1 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_4 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_5 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_6 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
inside_7 (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
mgmt (0 implicit incoming rules)
wifi (1 implicit incoming rule)
1 any Any less secure networks ip Permit Implicit rule: Permit all traffic to less secure netwo
Global (1 implicit rule)
1 any any ip Deny Implicit rule
Apply Reset Advanced...
Device List
Add Delete Connect
10.10.10.1
192.168.99.1
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Ethertype Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
VM Attribute Agent
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Addresses
Add Edit Delete Where Used Not Used
Network Objects
any
any4
any6
inside-network/24
mgmt-network/24
obj_any1
obj_any2
obj_any3
obj_any4
obj_any5
obj_any6
obj_any7
obj_any_wifi
PC1-network/24
PC2-network/24
WAN-network/24
wifi-network/24
Configuration changes saved successfully.
admin
16.02.23 16:46:48 UTC

Konfigurację interfejsów 2-8, aby **wszystkie** mogły ze sobą komunikować się niezależnie od security levelu, można zamiast w regułach firewalla skonfigurować również z konsoli. **Jest to niestosowane**, gdyż otwiera komunikację na wszystkich portach bez ograniczeń.

same-security-traffic permit intra-interface -> dla interfejsów o tym samych security level

same-security-traffic permit inter-interface -> umożliwia komunikację z poziomu niższego do wyższego

Interfejs 1 jest jako outside, bez reguł nie będzie komunikacji do niego, ani od niego