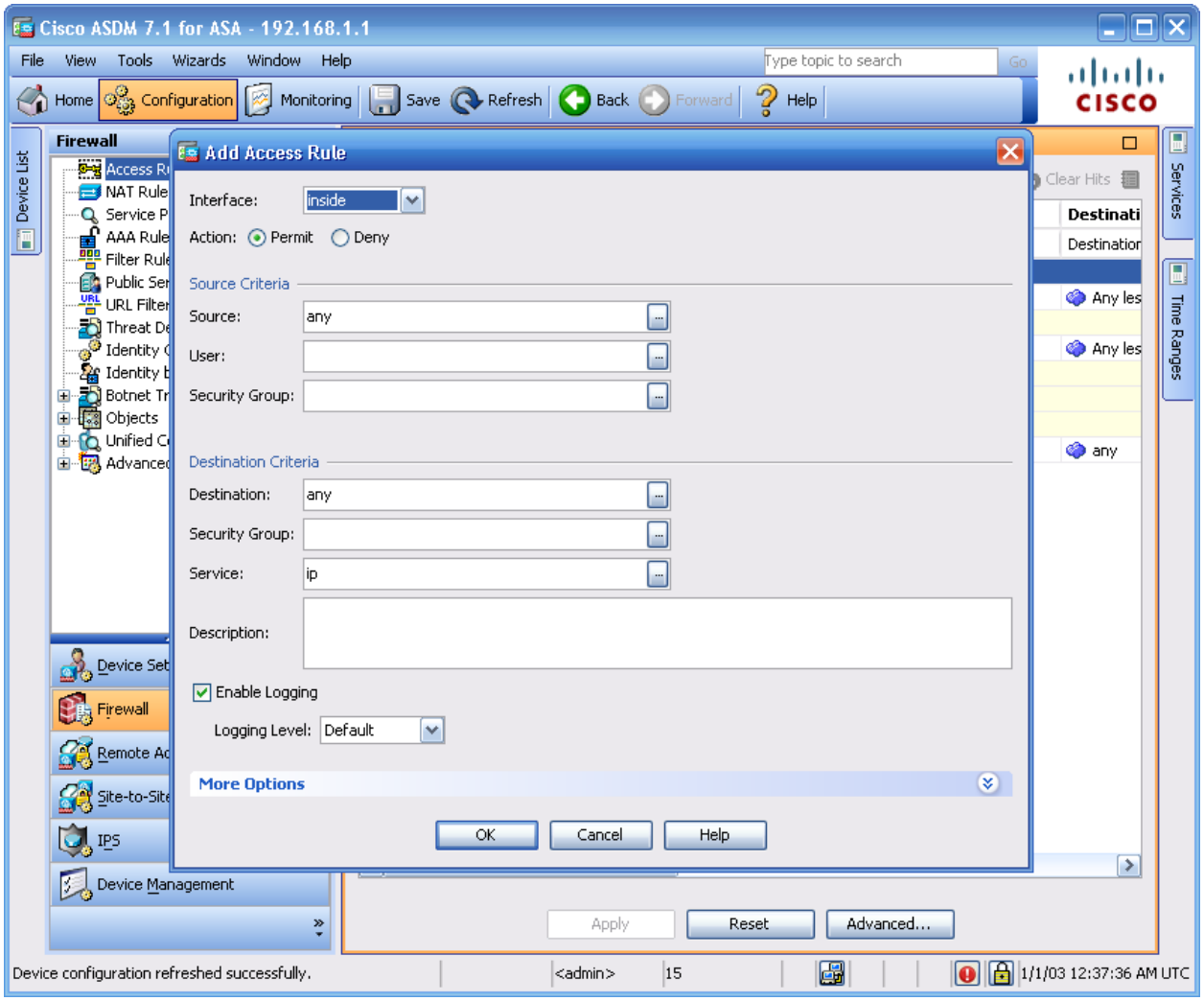
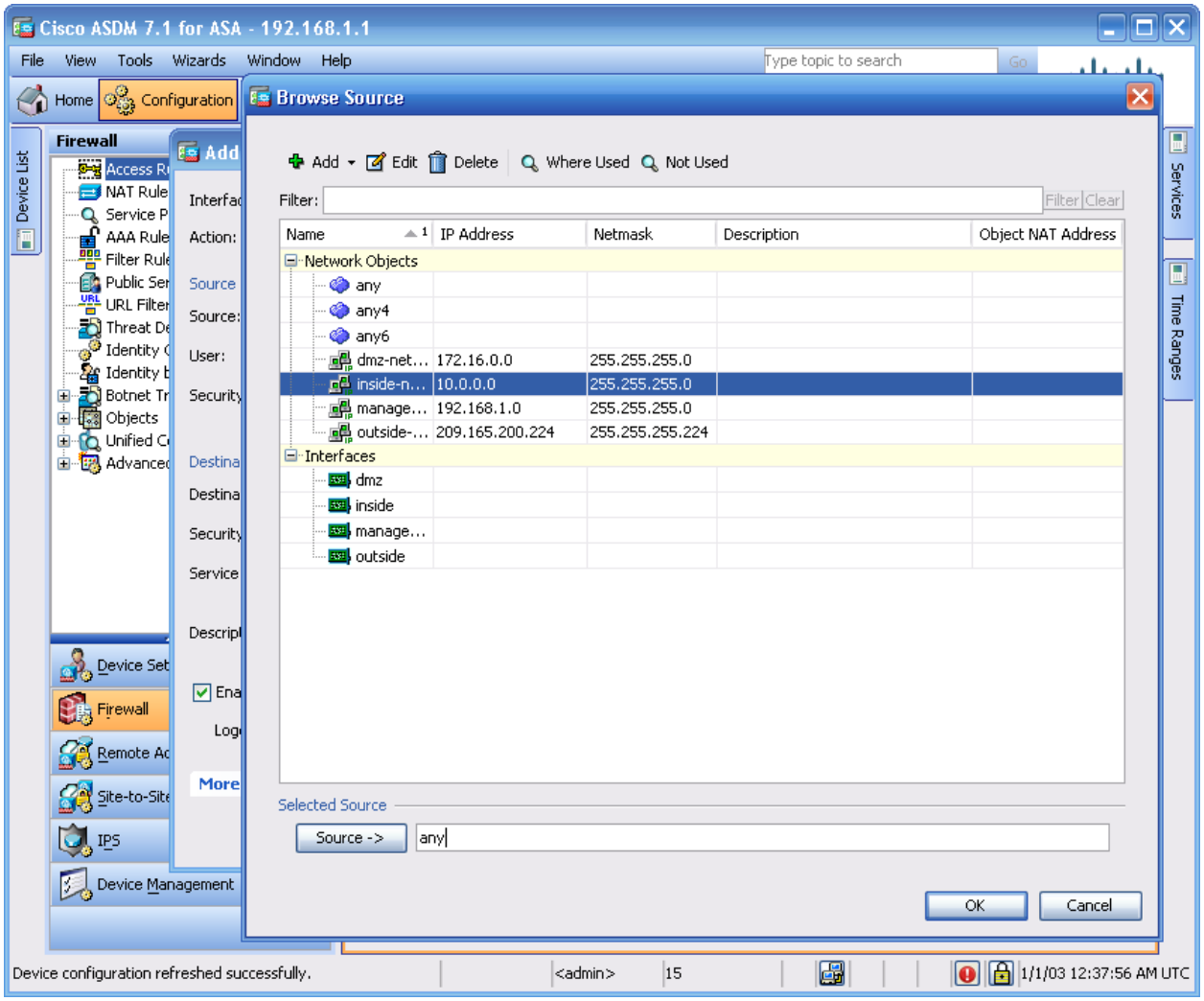
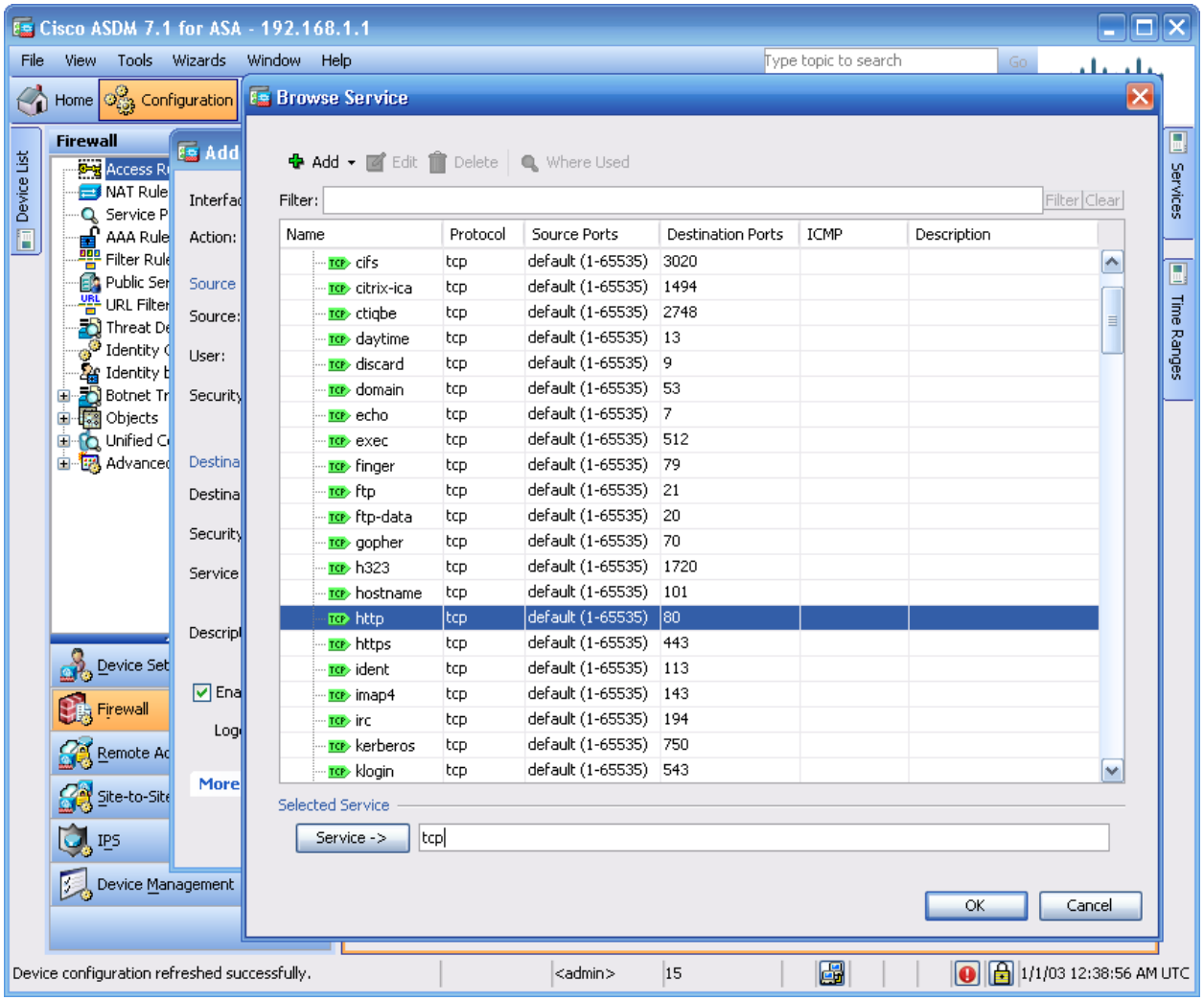
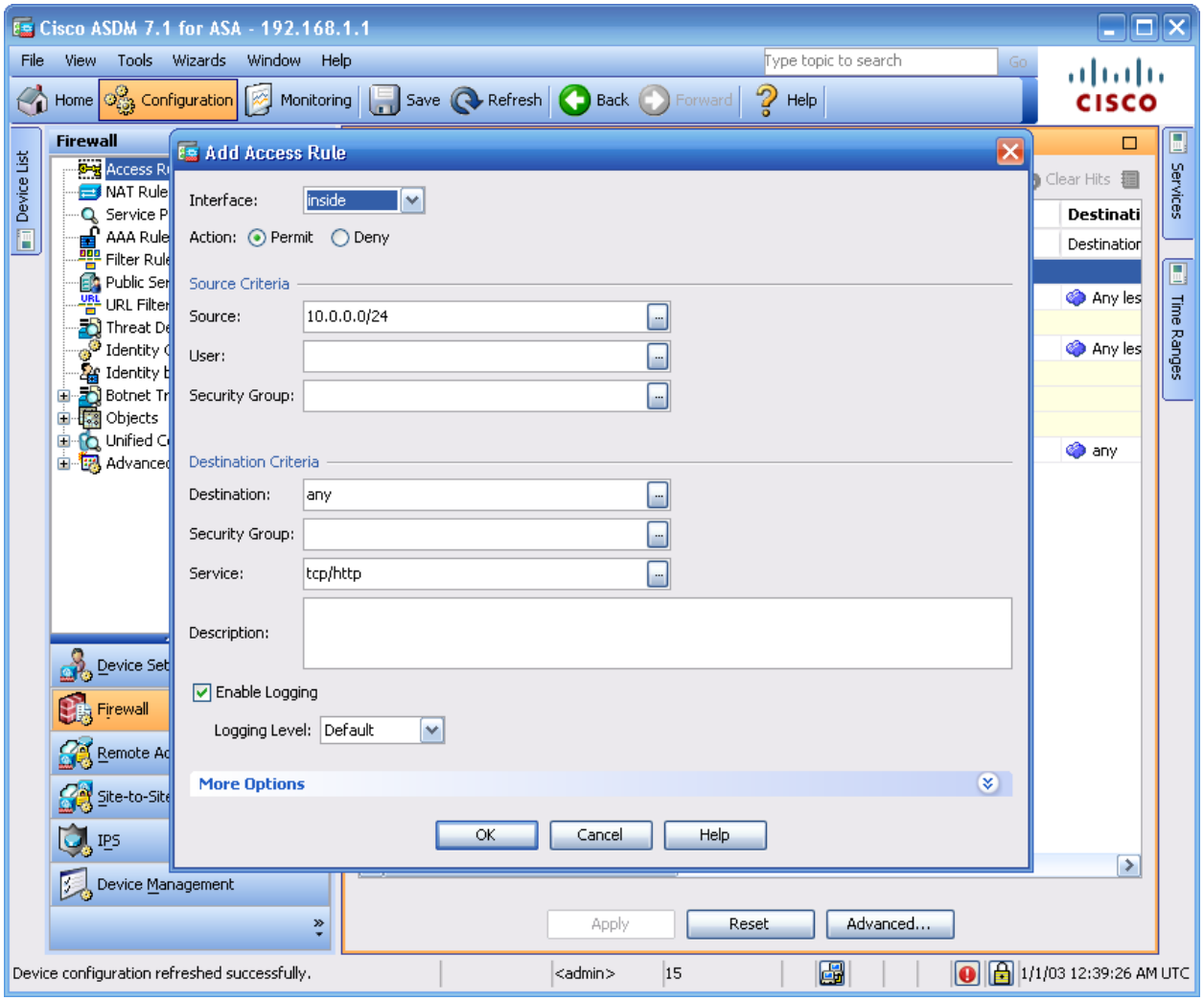
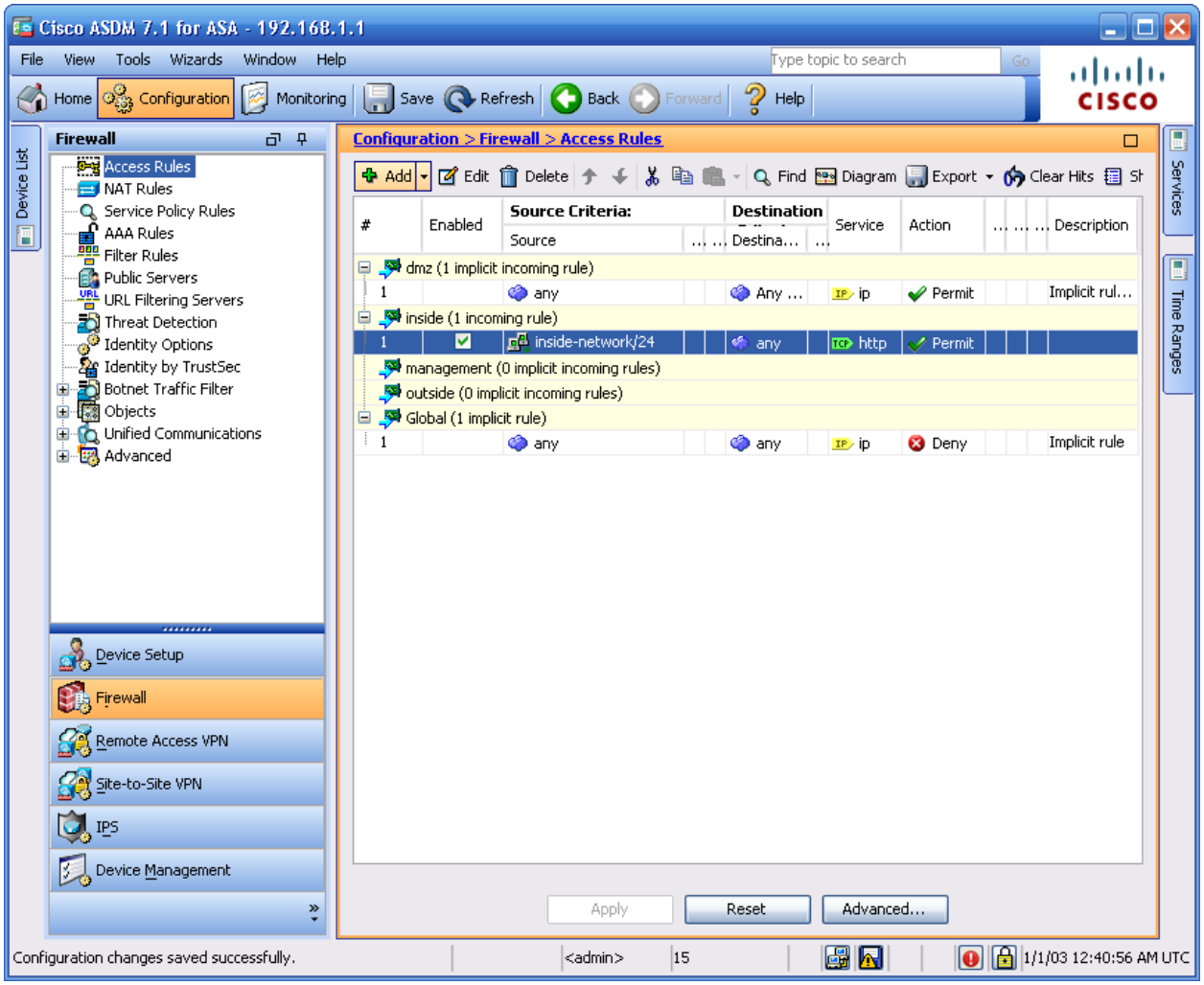
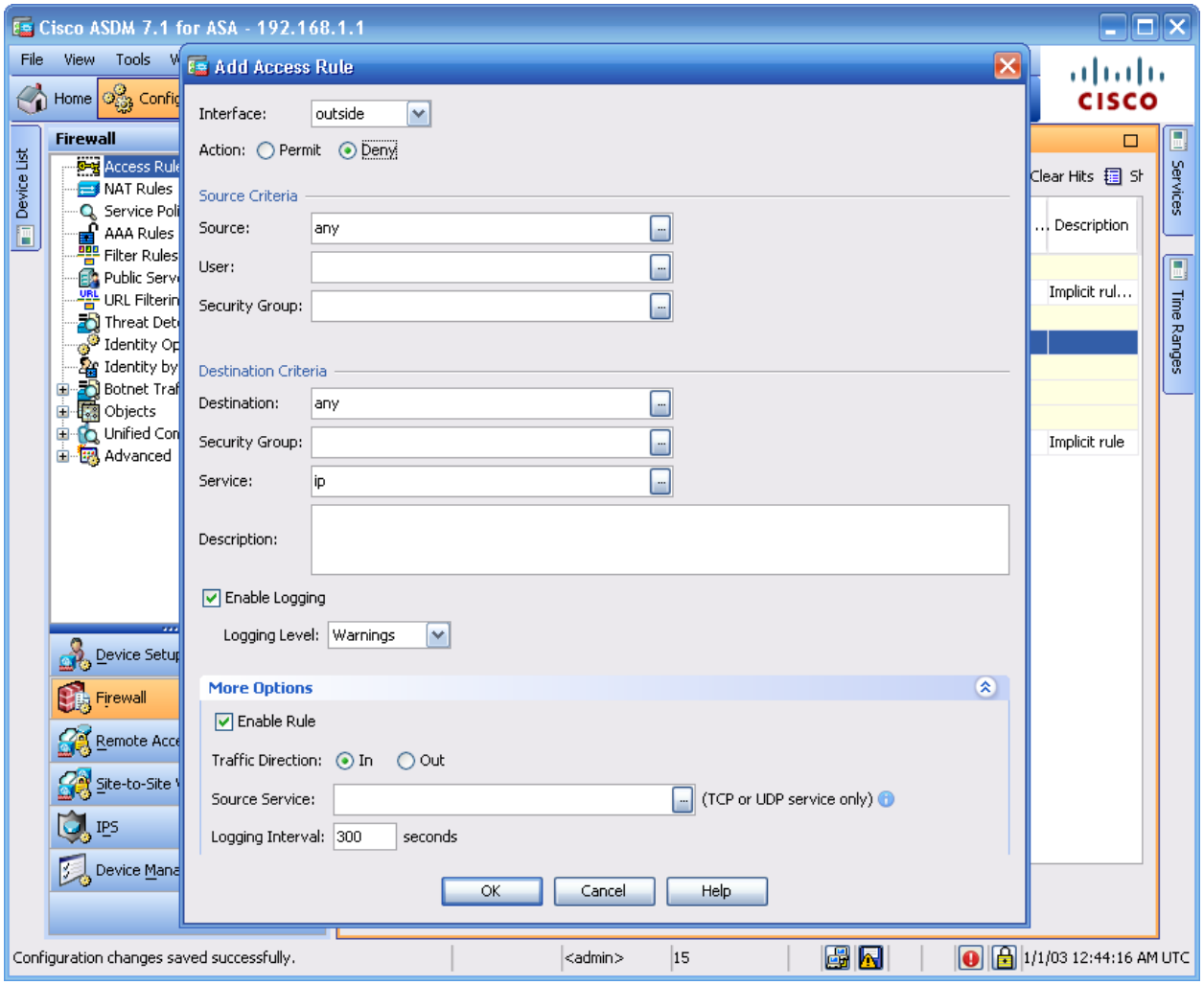

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Add Access Rule
Interface: inside
Action: Permit Deny
Source Criteria
Source: any
User:
Security Group:
Destination Criteria
Destination: any
Security Group:
Service: ip
Description:
Enable Logging
Logging Level: Default
More Options
OK Cancel Help
Firewall
Device Management
Apply Reset Advanced...
Device configuration refreshed successfully.
<admin> 15
1/1/03 12:37:36 AM UTC

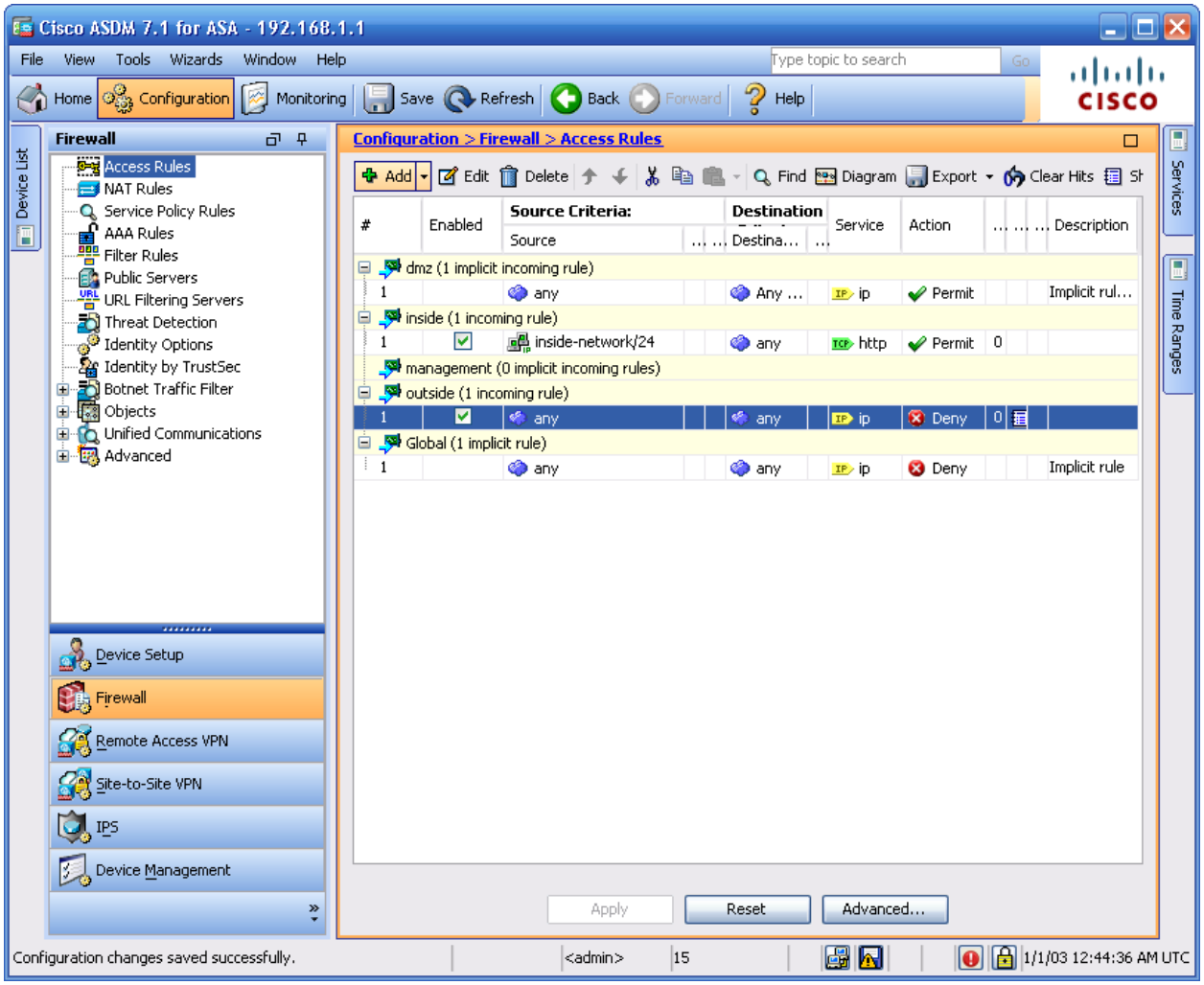

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home
Configuration
Browse Source
Add
Edit
Delete
Where Used
Not Used
Filter:
Filter
Clear
Name
IP Address
Netmask
Description
Object NAT Address
Network Objects
any
any4
any6
dmz-net...
172.16.0.0
255.255.255.0
inside-n...
10.0.0.0
255.255.255.0
manage...
192.168.1.0
255.255.255.0
outside-...
209.165.200.224
255.255.255.224
Interfaces
dmz
inside
manage...
outside
Selected Source
Source ->
any
OK
Cancel
Firewall
Device List
Services
Time Ranges
Device Configuration refreshed successfully.
<admin>
15
1/1/03 12:37:56 AM UTC

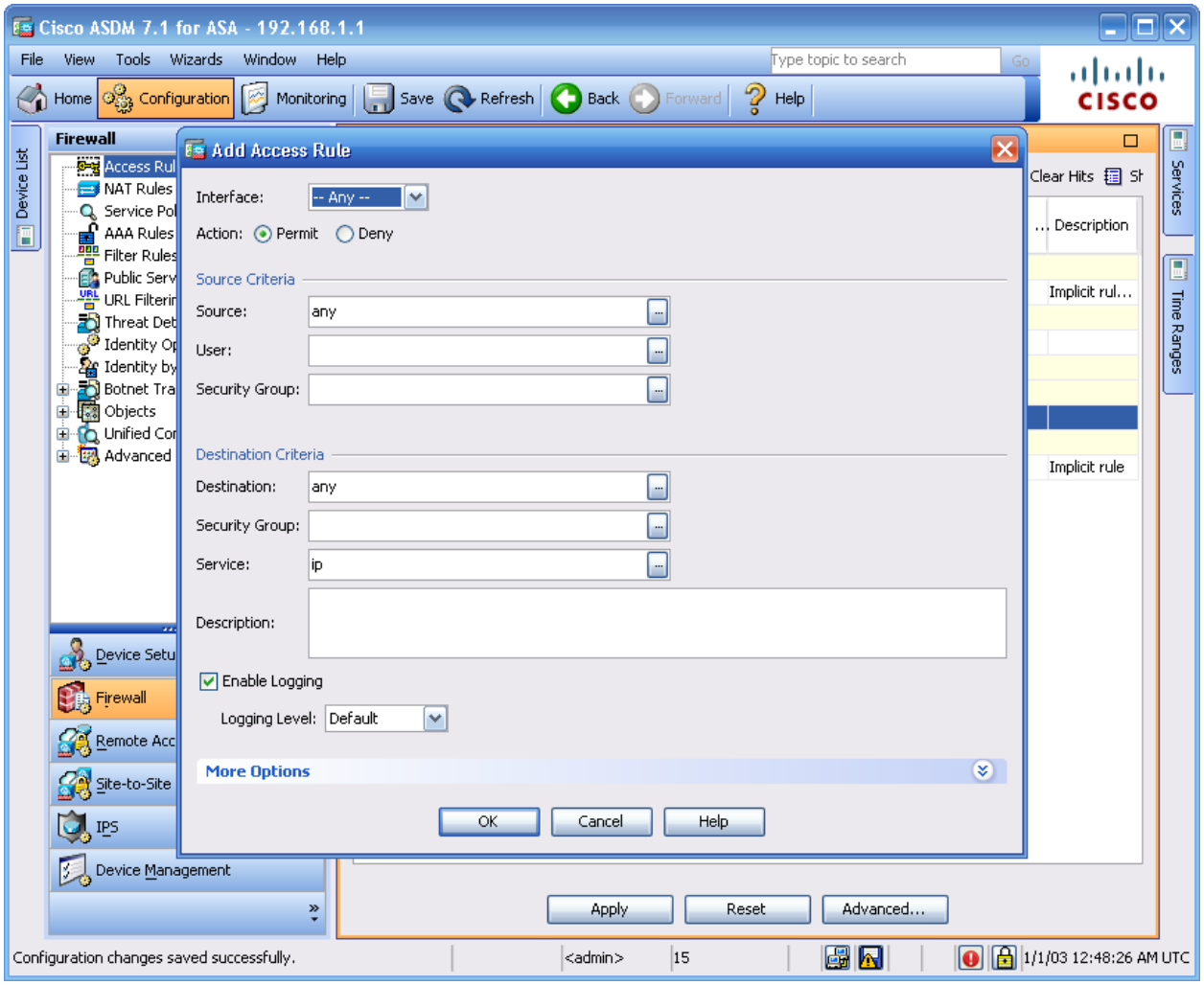

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home
Configuration
Browse Service
Add
Edit
Delete
Where Used
Filter:
Filter
Clear
Name
Protocol
Source Ports
Destination Ports
ICMP
Description
cifs tcp default (1-65535) 3020
citrix-ica tcp default (1-65535) 1494
ctiqbe tcp default (1-65535) 2748
daytime tcp default (1-65535) 13
discard tcp default (1-65535) 9
domain tcp default (1-65535) 53
echo tcp default (1-65535) 7
exec tcp default (1-65535) 512
finger tcp default (1-65535) 79
ftp tcp default (1-65535) 21
ftp-data tcp default (1-65535) 20
gopher tcp default (1-65535) 70
h323 tcp default (1-65535) 1720
hostname tcp default (1-65535) 101
http tcp default (1-65535) 80
https tcp default (1-65535) 443
ident tcp default (1-65535) 113
imap4 tcp default (1-65535) 143
irc tcp default (1-65535) 194
kerberos tcp default (1-65535) 750
klogin tcp default (1-65535) 543
Selected Service
Service ->
tcp
OK
Cancel
Device List
Services
Time Ranges
Firewall
Device Management
Device configuration refreshed successfully.
<admin>
15
1/1/03 12:38:56 AM UTC

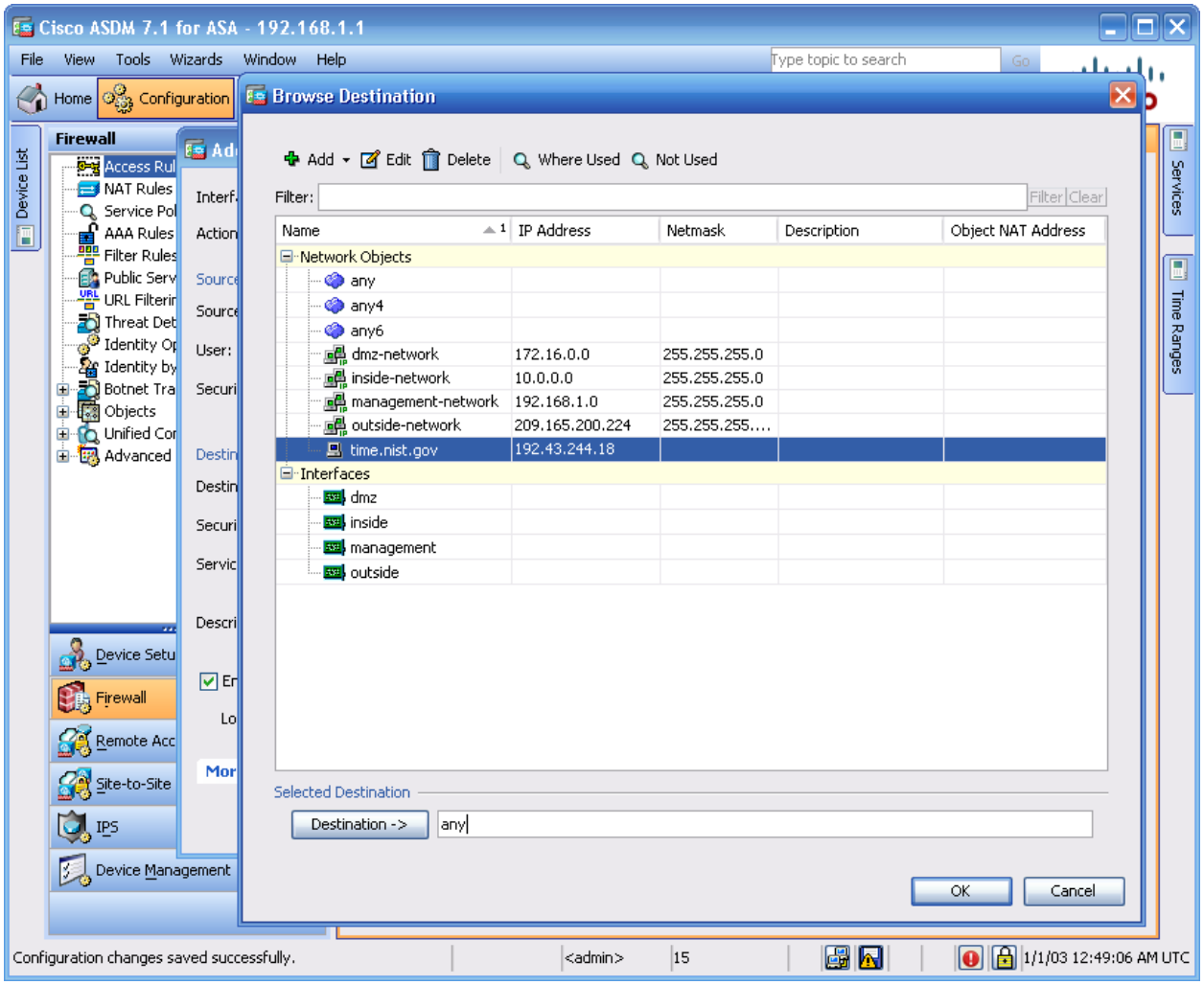

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Add Access Rule
Interface: inside
Action: Permit Deny
Source Criteria
Source: 10.0.0.0/24
User:
Security Group:
Destination Criteria
Destination: any
Security Group:
Service: tcp/http
Description:
Enable Logging
Logging Level: Default
More Options
OK Cancel Help
Firewall
Device Management
Apply Reset Advanced...
Device configuration refreshed successfully.
<admin> 15
1/1/03 12:39:26 AM UTC

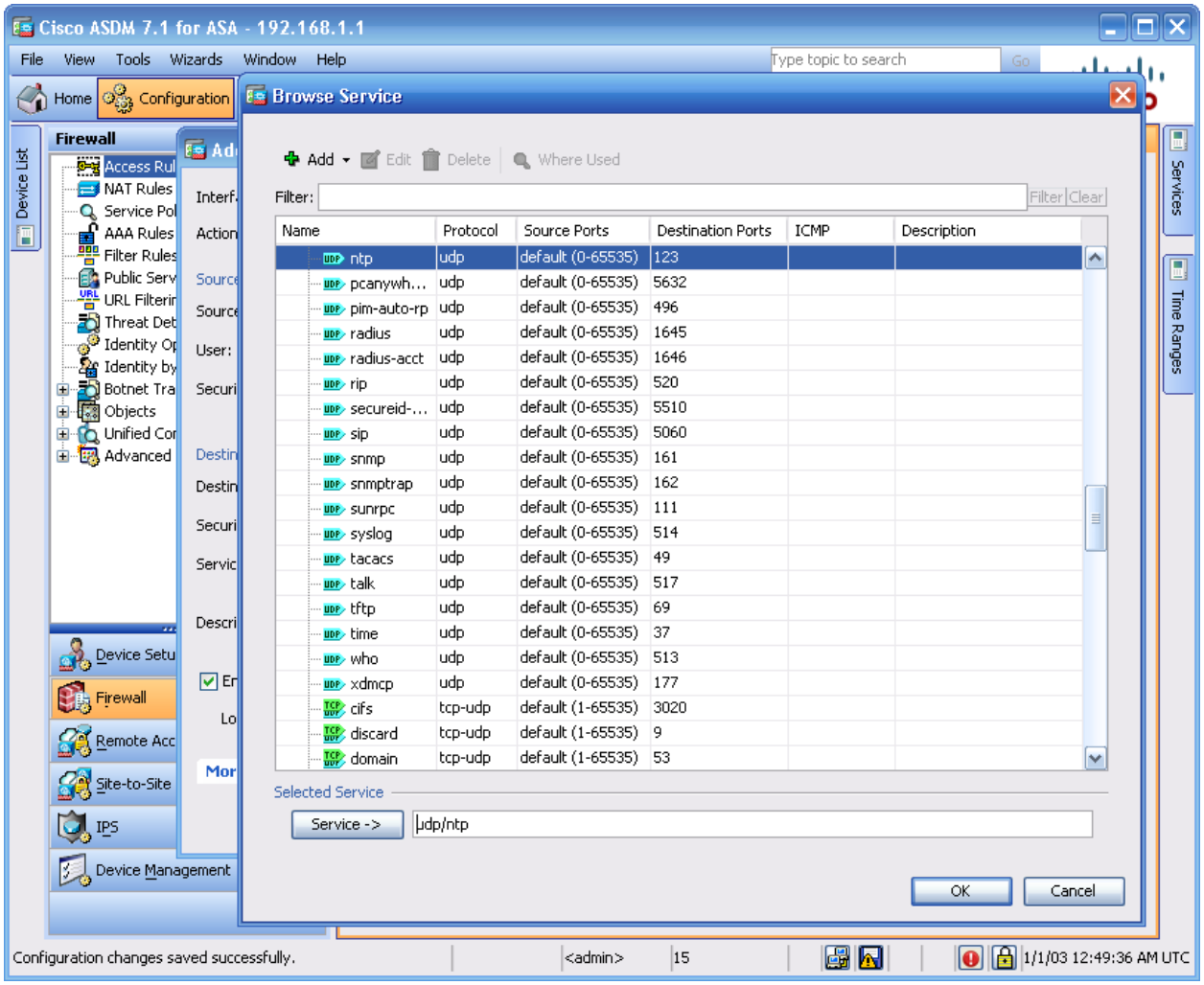

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits
Enabled Source Criteria: Source Destination Destina... Service Action Description
dmz (1 implicit incoming rule)
1 any Any ... ip Permit Implicit rul...
inside (1 incoming rule)
1 inside-network/24 any http Permit
management (0 implicit incoming rules)
outside (0 implicit incoming rules)
Global (1 implicit rule)
1 any any ip Deny Implicit rule
Apply Reset Advanced...
Device List
Services
Time Ranges
Configuration changes saved successfully.
<admin> 15
1/1/03 12:40:56 AM UTC

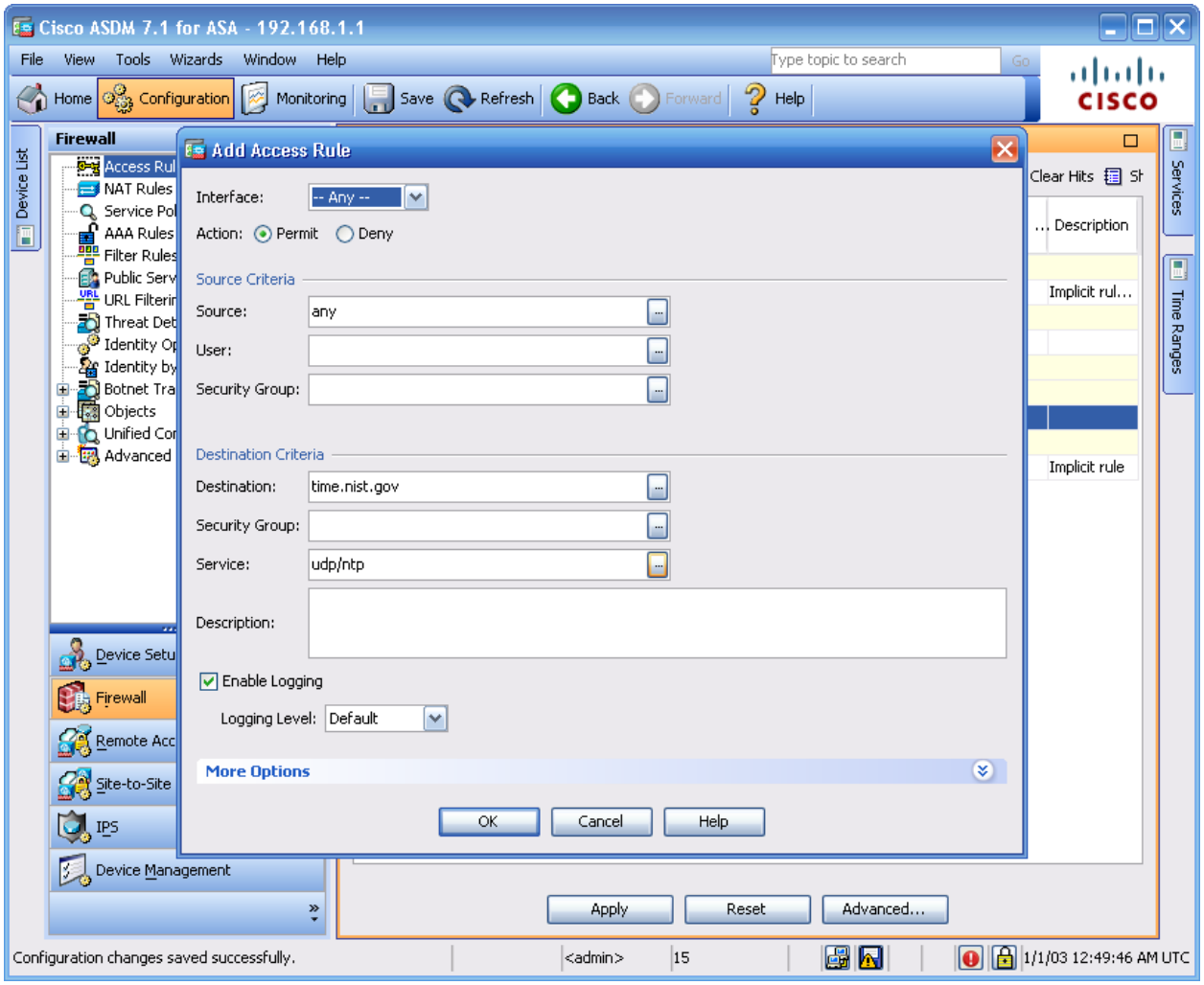

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools
Home
Firewall
Access Rule
NAT Rules
Service Poli
AAA Rules
Filter Rules
Public Serv
URL Filterin
Threat Det
Identity Op
Identity by
Botnet Traf
Objects
Unified Cor
Advanced
Device Setup
Firewall
Remote Acc
Site-to-Site
IPS
Device Mana
Device List
Add Access Rule
Interface: outside
Action: Permit Deny
Source Criteria
Source: any
User:
Security Group:
Destination Criteria
Destination: any
Security Group:
Service: ip
Description:
Enable Logging
Logging Level: Warnings
More Options
Enable Rule
Traffic Direction: In Out
Source Service: (TCP or UDP service only)
Logging Interval: 300 seconds
OK Cancel Help
Clear Hits
... Description
Implicit rul...
Implicit rule
Services
Time Ranges
Configuration changes saved successfully.
<admin>
15
1/1/03 12:44:16 AM UTC

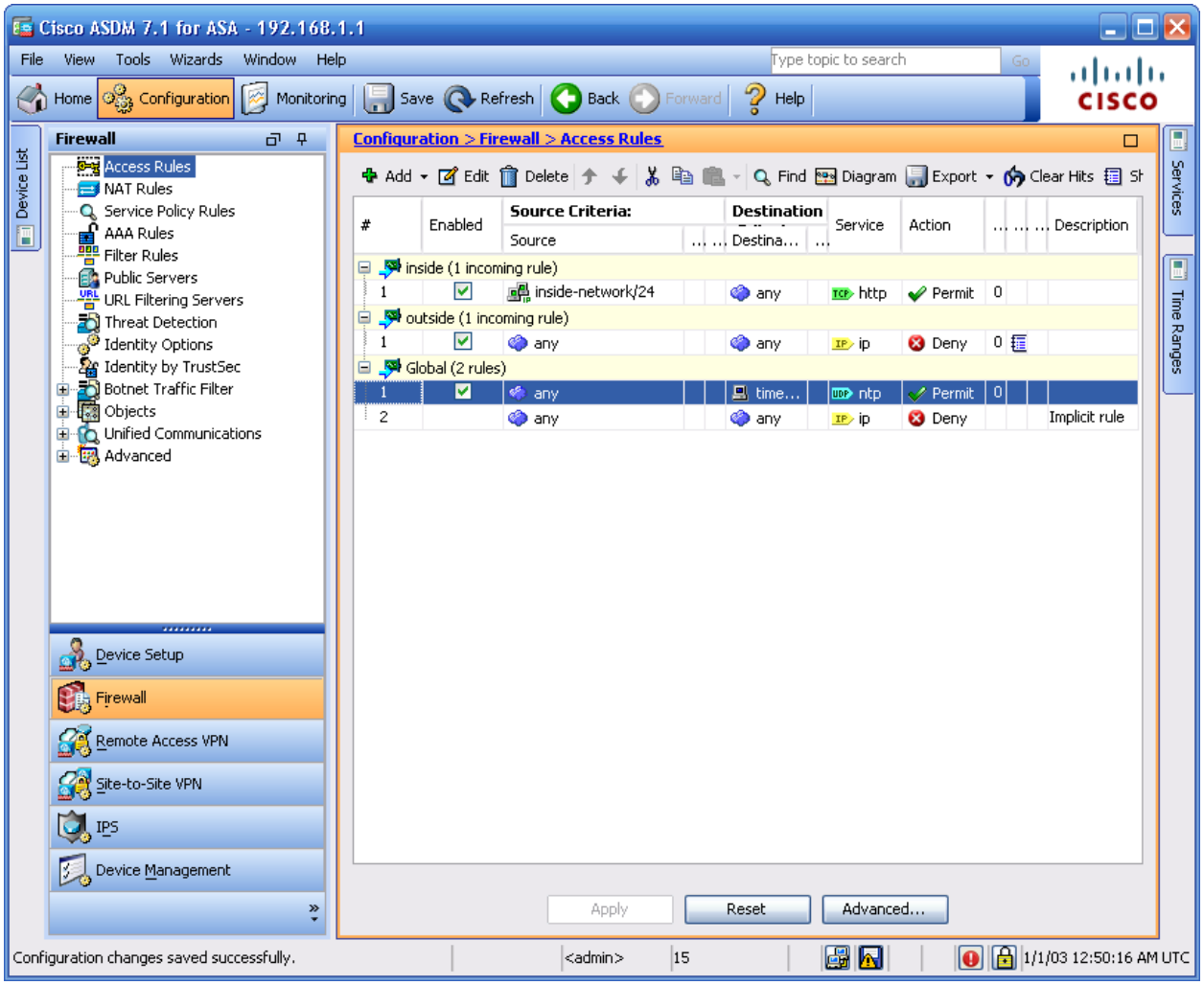

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits
Enabled Source Criteria: Source Destination Destina... Service Action Description
dmz (1 implicit incoming rule)
1 any Any ... ip Permit Implicit rul...
inside (1 incoming rule)
1 inside-network/24 any http Permit 0
management (0 implicit incoming rules)
outside (1 incoming rule)
1 any any ip Deny 0
Global (1 implicit rule)
1 any any ip Deny Implicit rule
Apply Reset Advanced...
Services
Time Ranges
Configuration changes saved successfully.
<admin> 15
1/1/03 12:44:36 AM UTC

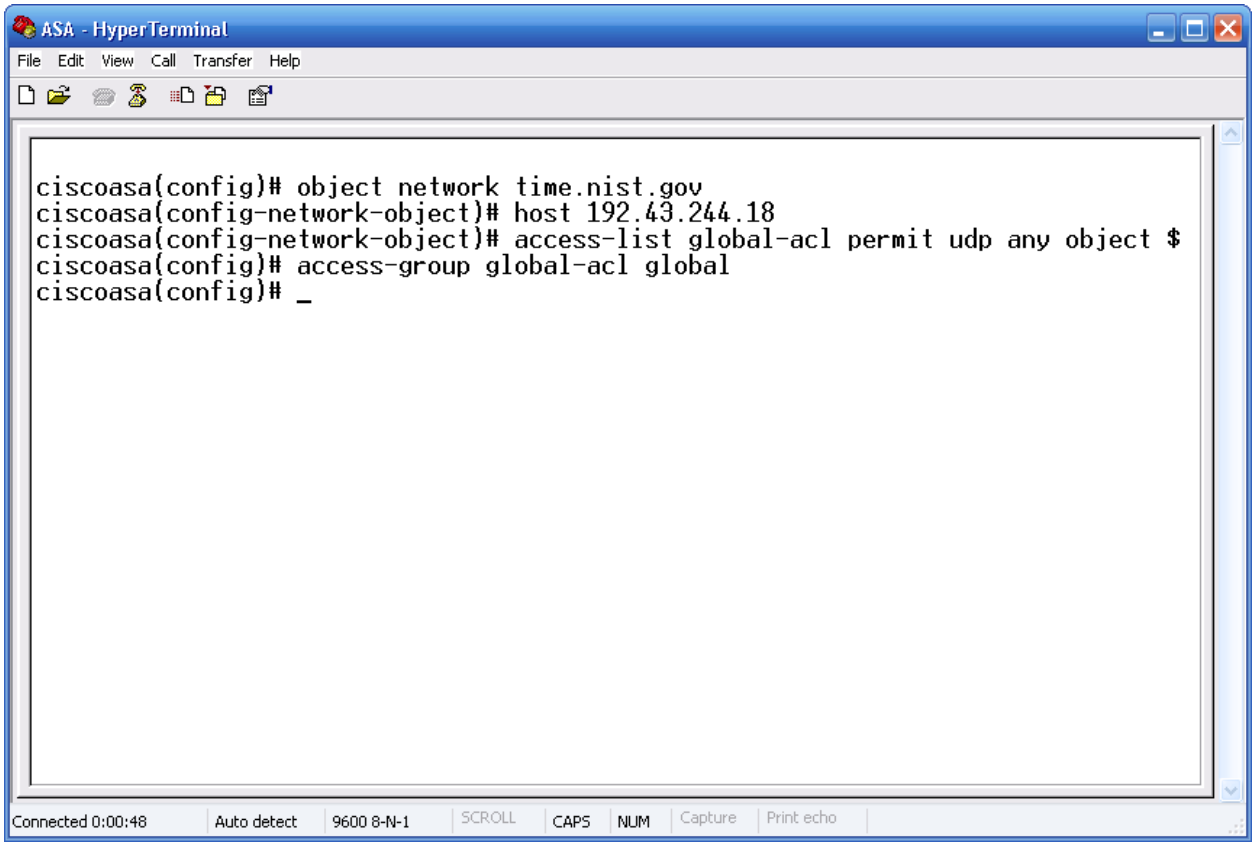

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rul
NAT Rules
Service Pol
AAA Rules
Filter Rules
Public Serv
URL Filterir
Threat Det
Identity Op
Identity by
Botnet Tra
Objects
Unified Cor
Advanced
Device Setu
Firewall
Remote Acc
Site-to-Site
IPS
Device Management
Add Access Rule
Interface: -- Any --
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
OK Cancel Help
Clear Hits
... Description
Implicit rul...
Implicit rule
Apply Reset Advanced...
Device List
Services
Time Ranges
Configuration changes saved successfully.
<admin> 15
1/1/03 12:48:26 AM UTC

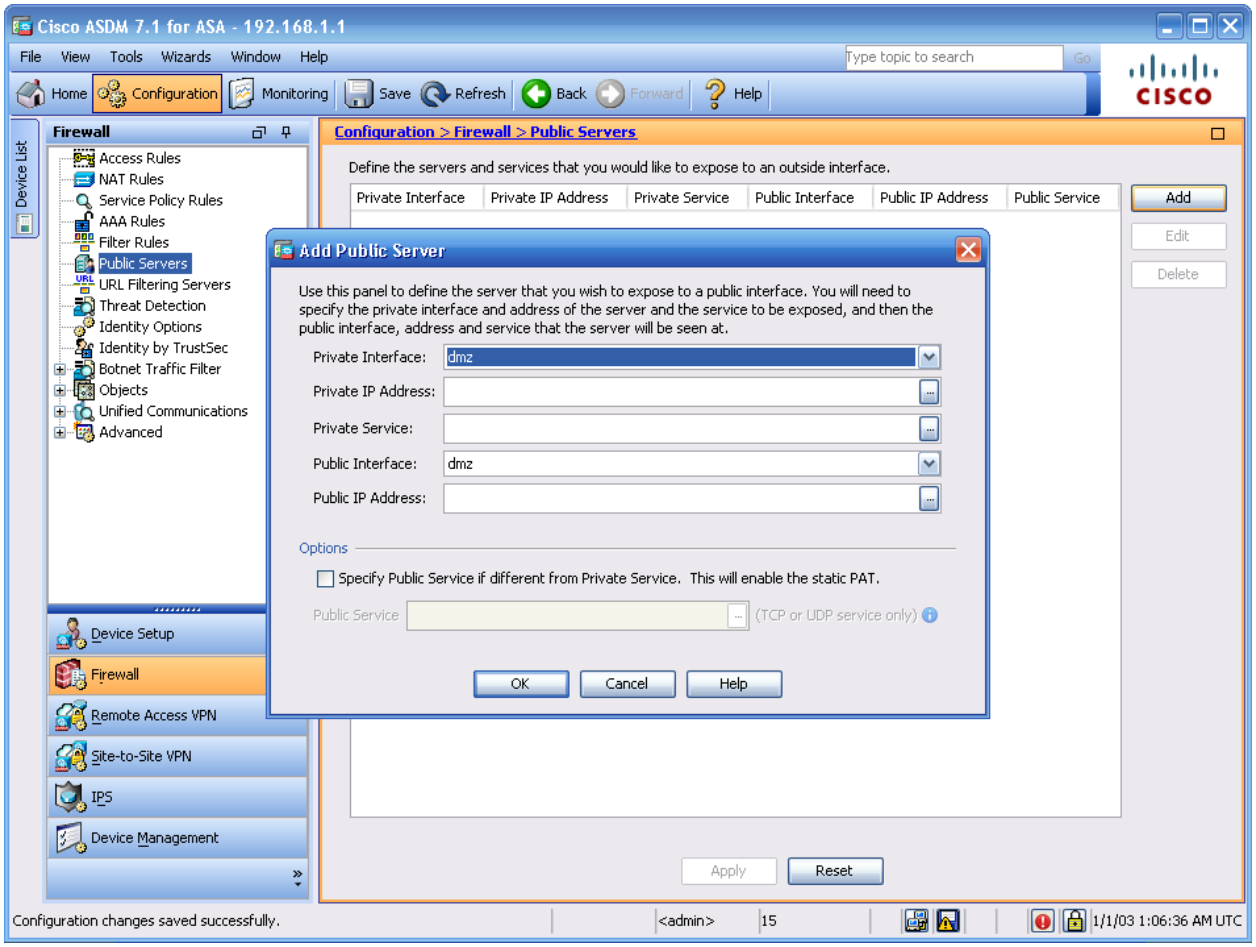

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration
Browse Destination
Add Edit Delete Where Used Not Used
Filter: Filter Clear
Name IP Address Netmask Description Object NAT Address
Network Objects
any
any4
any6
dmz-network 172.16.0.0 255.255.255.0
inside-network 10.0.0.0 255.255.255.0
management-network 192.168.1.0 255.255.255.0
outside-network 209.165.200.224 255.255.255....
time.nist.gov 192.43.244.18
Interfaces
dmz
inside
management
outside
Selected Destination
Destination -> any
OK Cancel
Firewall
Access Rul
NAT Rules
Service Pol
AAA Rules
Filter Rules
Public Serv
URL Filterir
Threat Det
Identity Op
Identity by
Botnet Tra
Objects
Unified Cor
Advanced
Device Setu
Firewall
Remote Acc
Site-to-Site
IPS
Device Management
Device List
Services
Time Ranges
Configuration changes saved successfully.
<admin>
15
1/1/03 12:49:06 AM UTC

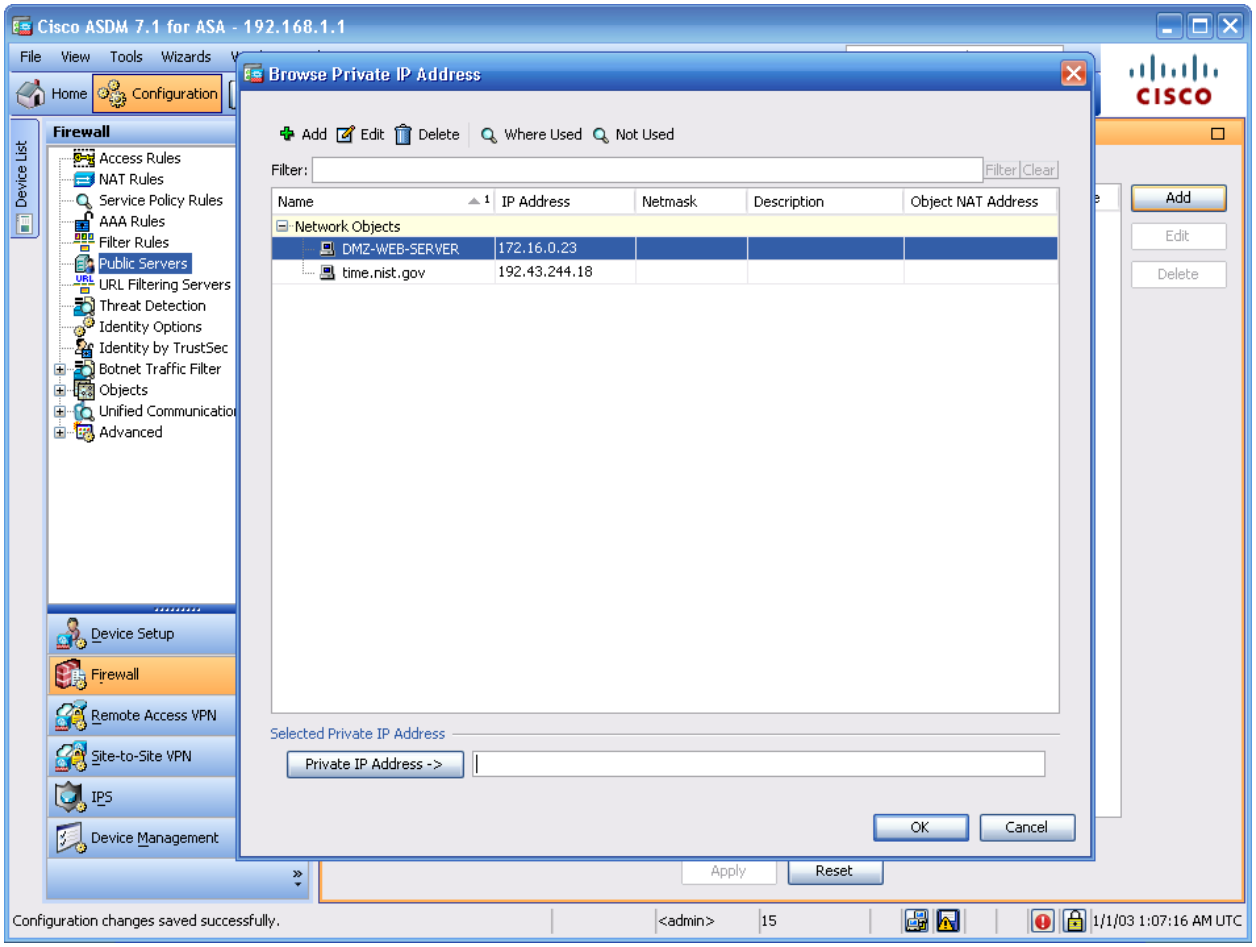

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration
Browse Service
Add Edit Delete Where Used
Filter: Filter Clear
Name Protocol Source Ports Destination Ports ICMP Description
ntp udp default (0-65535) 123
pcanywh... udp default (0-65535) 5632
pim-auto-rp udp default (0-65535) 496
radius udp default (0-65535) 1645
radius-acct udp default (0-65535) 1646
rip udp default (0-65535) 520
secureid-... udp default (0-65535) 5510
sip udp default (0-65535) 5060
snmp udp default (0-65535) 161
snmptrap udp default (0-65535) 162
sunrpc udp default (0-65535) 111
syslog udp default (0-65535) 514
tacacs udp default (0-65535) 49
talk udp default (0-65535) 517
tftp udp default (0-65535) 69
time udp default (0-65535) 37
who udp default (0-65535) 513
xdmcp udp default (0-65535) 177
cifs tcp-udp default (1-65535) 3020
discard tcp-udp default (1-65535) 9
domain tcp-udp default (1-65535) 53
Selected Service
Service -> udp/ntp
OK Cancel
Firewall
Device List
Services
Time Ranges
Configuration changes saved successfully.
<admin> 15
1/1/03 12:49:36 AM UTC

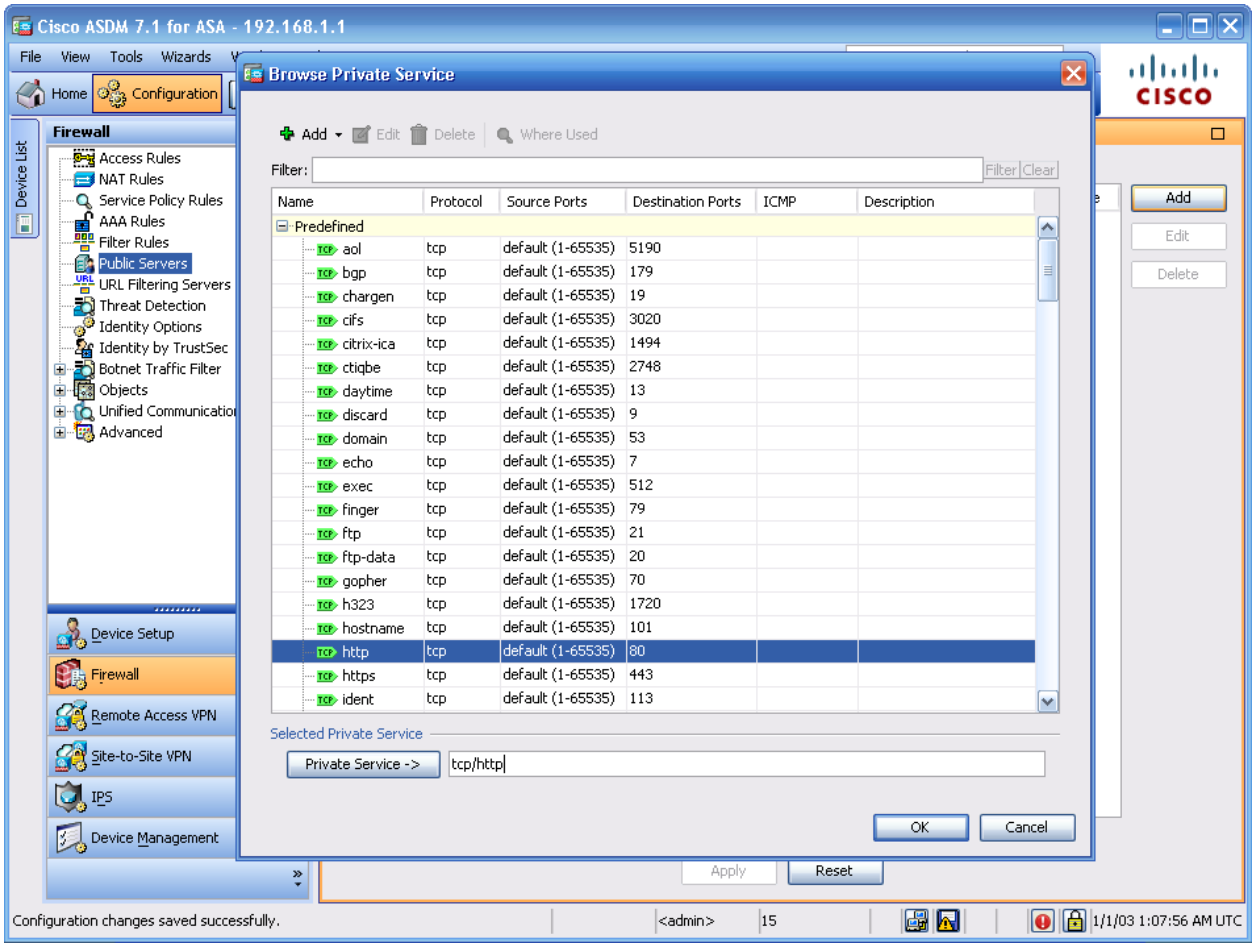

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rul
NAT Rules
Service Pol
AAA Rules
Filter Rules
Public Serv
URL Filterir
Threat Det
Identity Op
Identity by
Botnet Tra
Objects
Unified Cor
Advanced
Device Setu
Firewall
Remote Acc
Site-to-Site
IPS
Device Management
Add Access Rule
Interface: -- Any --
Action: Permit Deny
Source Criteria
Source: any
User:
Security Group:
Destination Criteria
Destination: time.nist.gov
Security Group:
Service: udp/ntp
Description:
Enable Logging
Logging Level: Default
More Options
OK Cancel Help
Clear Hits
... Description
Implicit rul...
Implicit rule
Apply Reset Advanced...
Device List
Services
Time Ranges
Configuration changes saved successfully.
<admin>
15
1/1/03 12:49:46 AM UTC

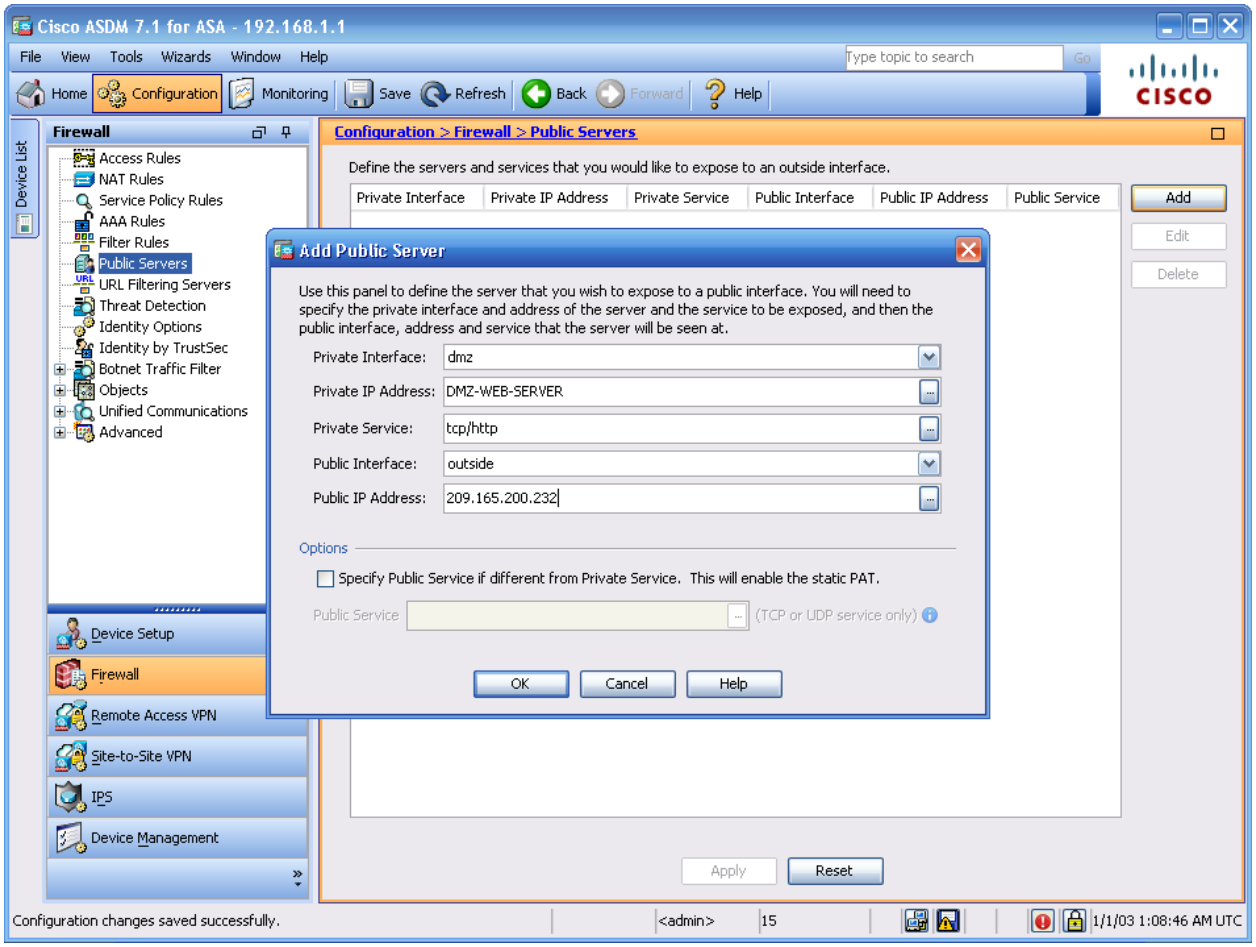

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits
Enabled Source Criteria: Source Destination Service Action Description
inside (1 incoming rule)
1 inside-network/24 any http Permit 0
outside (1 incoming rule)
1 any any ip Deny 0
Global (2 rules)
1 any time... ntp Permit 0
2 any any ip Deny Implicit rule
Apply Reset Advanced...
Services
Time Ranges
Configuration changes saved successfully.
<admin> 15
1/1/03 12:50:16 AM UTC

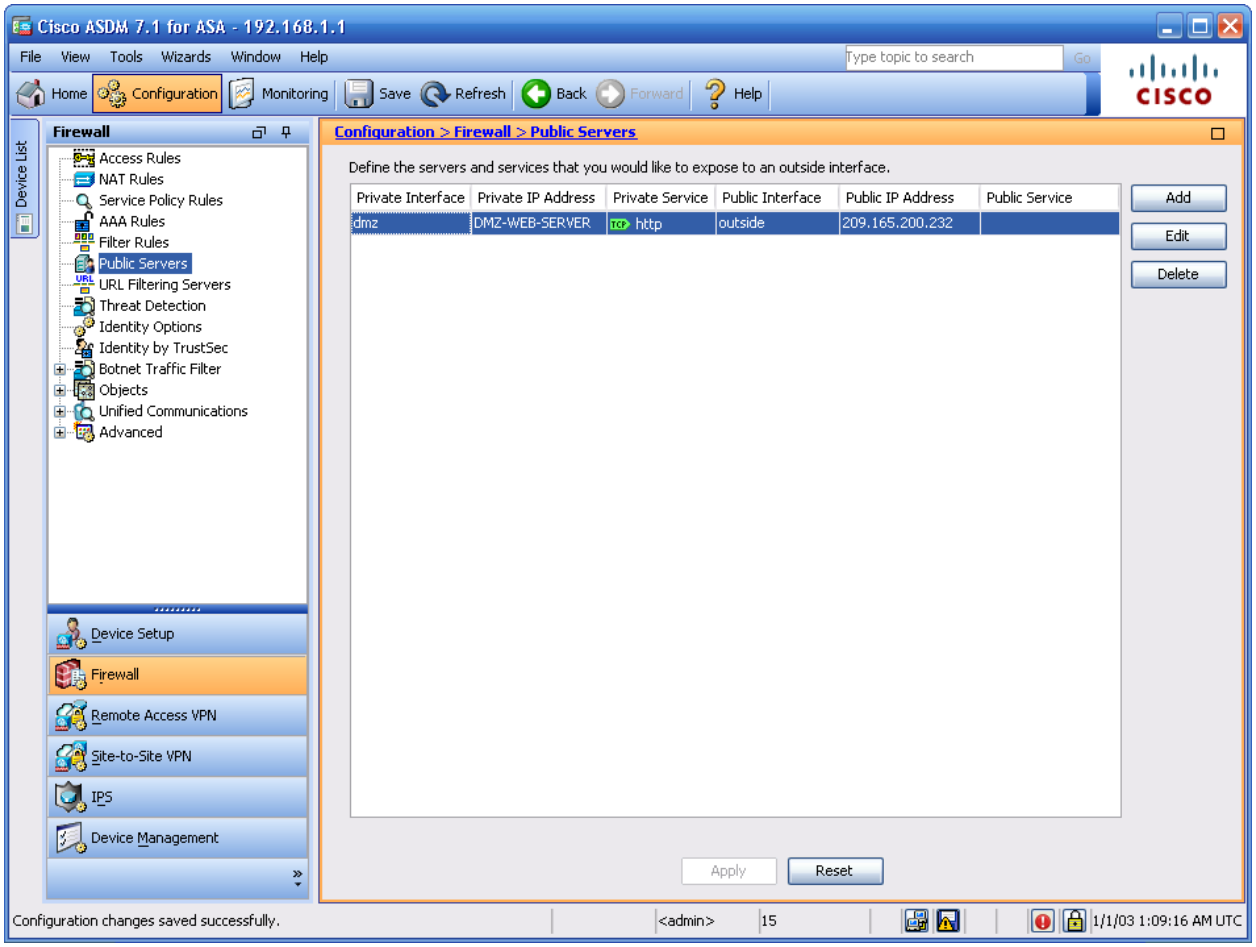

ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# object network time.nist.gov
ciscoasa(config-network-object)# host 192.43.244.18
ciscoasa(config-network-object)# access-list global-acl permit udp any object $
ciscoasa(config)# access-group global-acl global
ciscoasa(config)# _
Connected 0:00:48
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

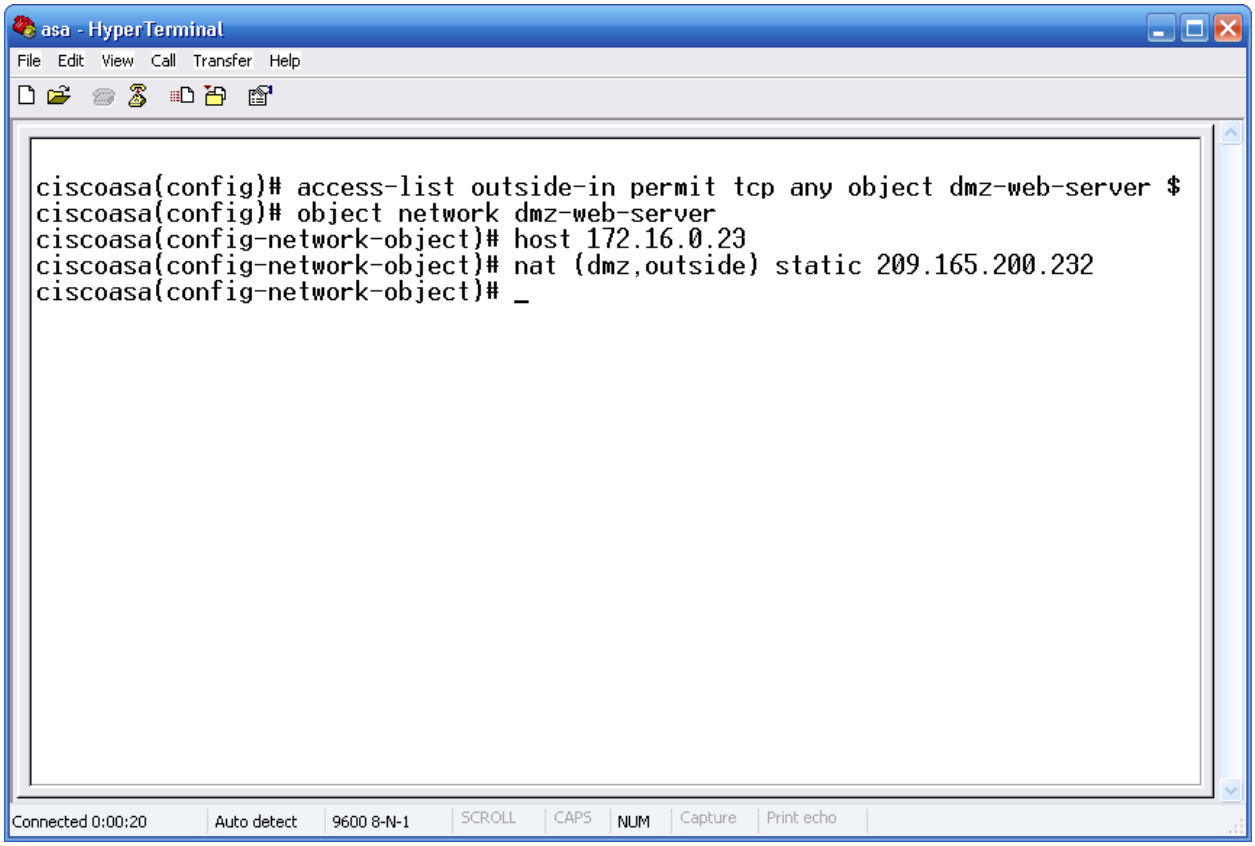

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Public Servers
Define the servers and services that you would like to expose to an outside interface.
Private Interface
Private IP Address
Private Service
Public Interface
Public IP Address
Public Service
Add
Edit
Delete
Add Public Server
Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface and address of the server and the service to be exposed, and then the public interface, address and service that the server will be seen at.
Private Interface: dmz
Private IP Address:
Private Service:
Public Interface: dmz
Public IP Address:
Options
Specify Public Service if different from Private Service. This will enable the static PAT.
Public Service
(TCP or UDP service only)
OK
Cancel
Help
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:06:36 AM UTC

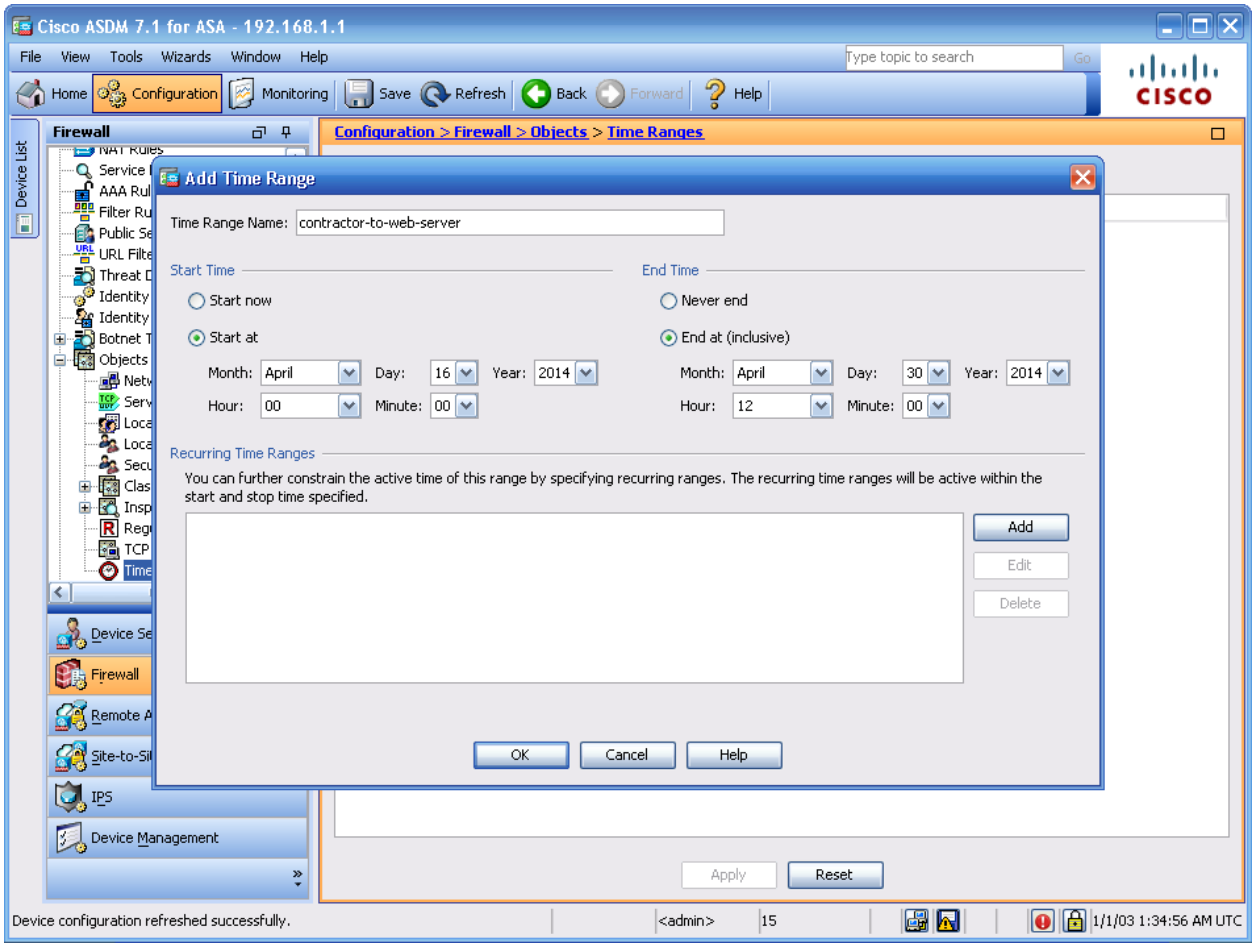

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards
Home Configuration
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communicatio
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Browse Private IP Address
Add Edit Delete Where Used Not Used
Filter:
Filter Clear
Name
IP Address
Netmask
Description
Object NAT Address
Network Objects
DMZ-WEB-SERVER
172.16.0.23
time.nist.gov
192.43.244.18
Selected Private IP Address
Private IP Address ->
OK
Cancel
Add
Edit
Delete
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:07:16 AM UTC

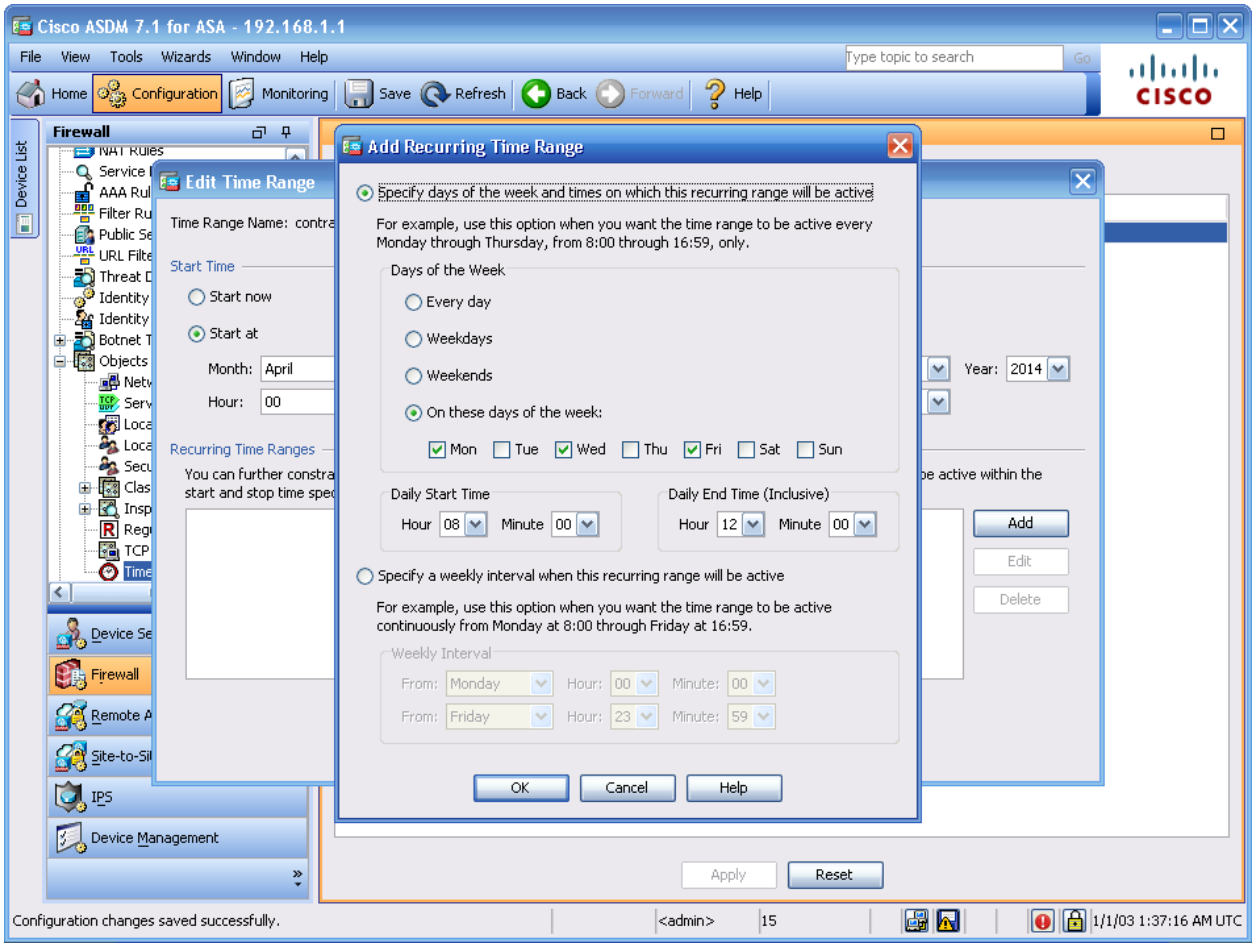

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards
Home Configuration
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communicatio
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Browse Private Service
Add Edit Delete Where Used
Filter: Filter Clear
Name Protocol Source Ports Destination Ports ICMP Description
Predefined
aol tcp default (1-65535) 5190
bgp tcp default (1-65535) 179
chargen tcp default (1-65535) 19
cifs tcp default (1-65535) 3020
citrix-ica tcp default (1-65535) 1494
ctiqbe tcp default (1-65535) 2748
daytime tcp default (1-65535) 13
discard tcp default (1-65535) 9
domain tcp default (1-65535) 53
echo tcp default (1-65535) 7
exec tcp default (1-65535) 512
finger tcp default (1-65535) 79
ftp tcp default (1-65535) 21
ftp-data tcp default (1-65535) 20
gopher tcp default (1-65535) 70
h323 tcp default (1-65535) 1720
hostname tcp default (1-65535) 101
http tcp default (1-65535) 80
https tcp default (1-65535) 443
ident tcp default (1-65535) 113
Selected Private Service
Private Service ->
tcp/http
OK
Cancel
Add
Edit
Delete
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:07:56 AM UTC

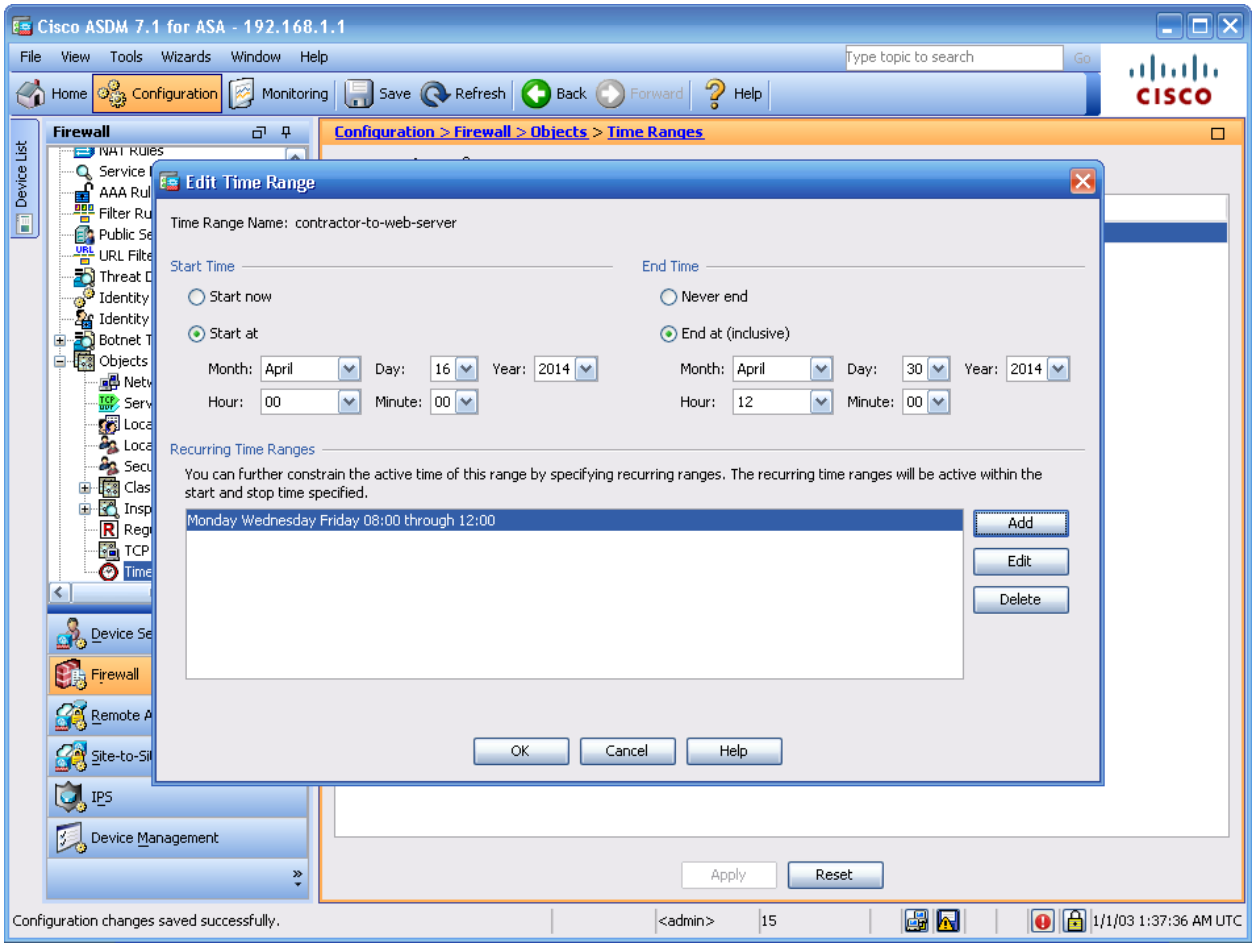

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Public Servers
Define the servers and services that you would like to expose to an outside interface.
Private Interface
Private IP Address
Private Service
Public Interface
Public IP Address
Public Service
Add
Edit
Delete
Add Public Server
Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface and address of the server and the service to be exposed, and then the public interface, address and service that the server will be seen at.
Private Interface: dmz
Private IP Address: DMZ-WEB-SERVER
Private Service: tcp/http
Public Interface: outside
Public IP Address: 209.165.200.232
Options
Specify Public Service if different from Private Service. This will enable the static PAT.
Public Service
(TCP or UDP service only)
OK
Cancel
Help
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:08:46 AM UTC

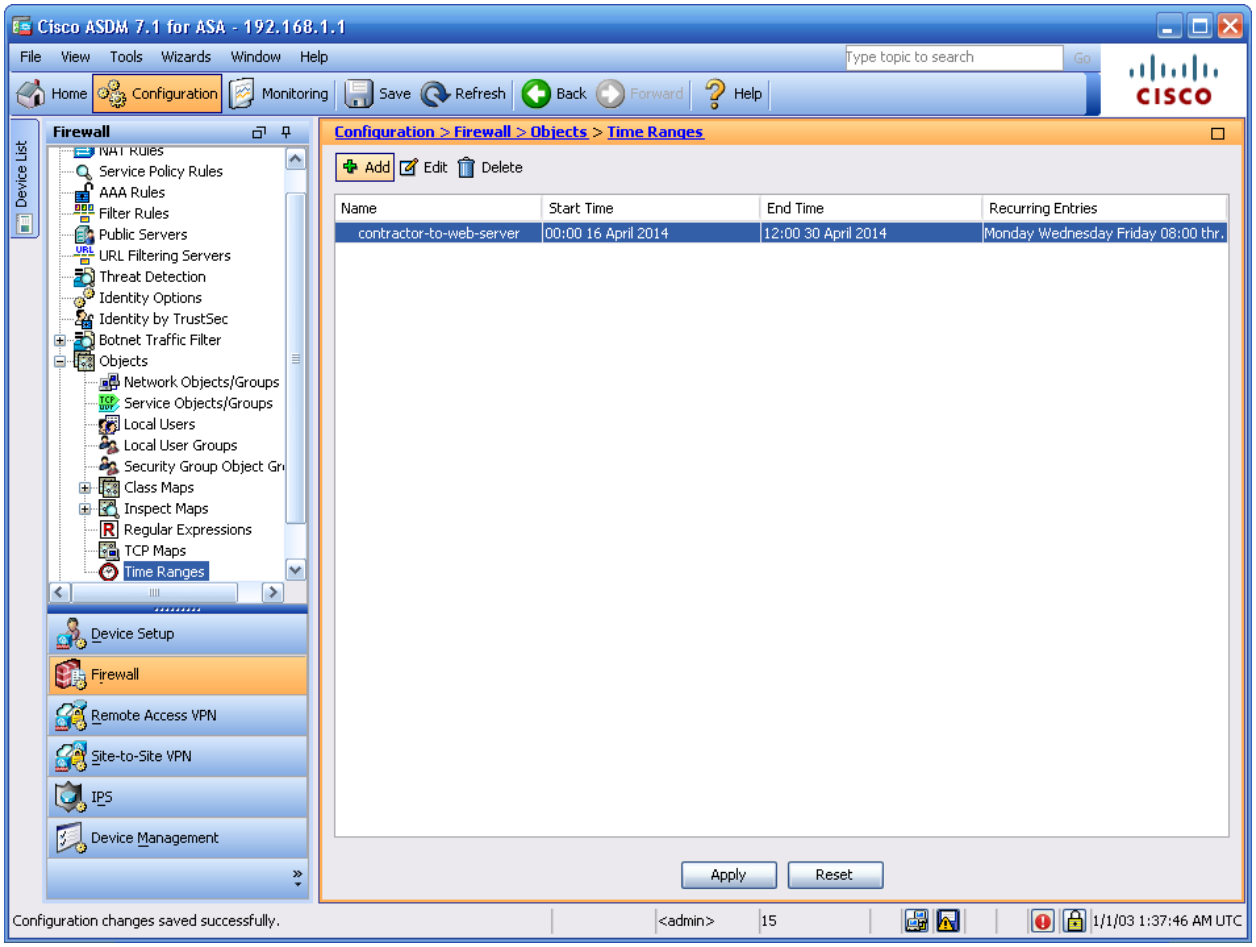

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
cisco
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Public Servers
Define the servers and services that you would like to expose to an outside interface.
Private Interface
Private IP Address
Private Service
Public Interface
Public IP Address
Public Service
dmz
DMZ-WEB-SERVER
http
outside
209.165.200.232
Add
Edit
Delete
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:09:16 AM UTC

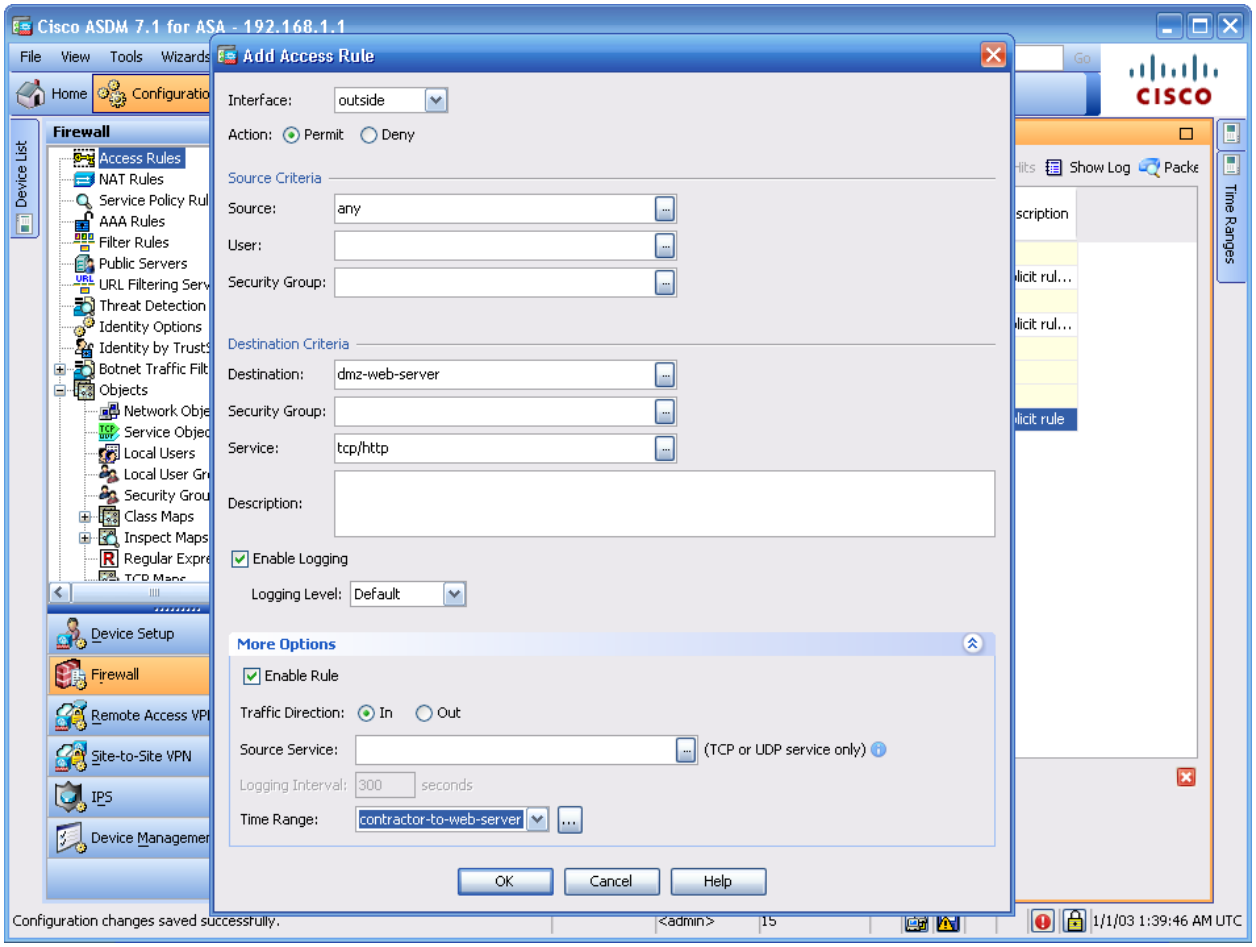

asa - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# access-list outside-in permit tcp any object dmz-web-server $
ciscoasa(config)# object network dmz-web-server
ciscoasa(config-network-object)# host 172.16.0.23
ciscoasa(config-network-object)# nat (dmz,outside) static 209.165.200.232
ciscoasa(config-network-object)# _
Connected 0:00:20
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

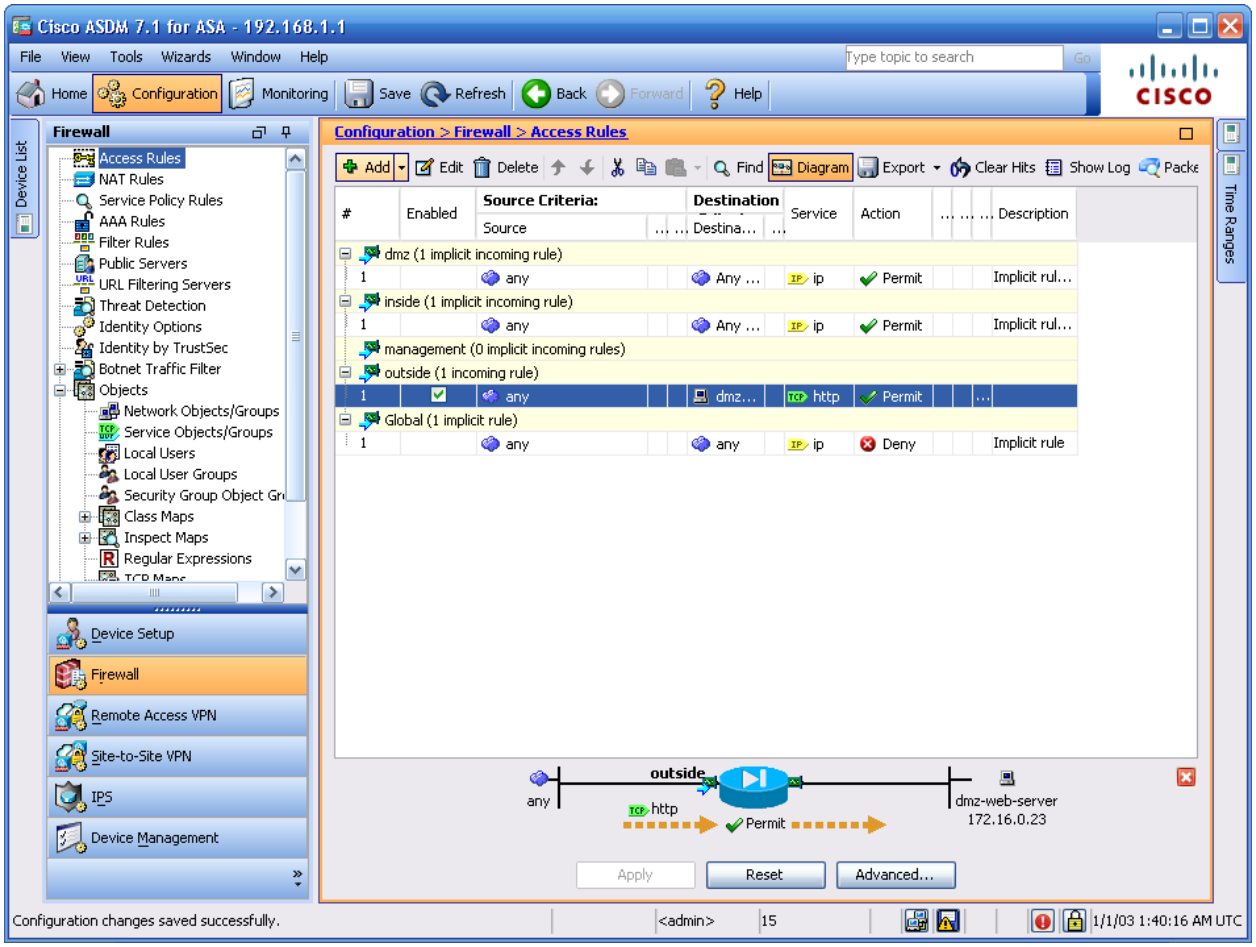

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Firewall
Configuration > Firewall > Objects > Time Ranges
Add Time Range
Time Range Name: contractor-to-web-server
Start Time
Start now
Start at
Month: April Day: 16 Year: 2014
Hour: 00 Minute: 00
End Time
Never end
End at (inclusive)
Month: April Day: 30 Year: 2014
Hour: 12 Minute: 00
Recurring Time Ranges
You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.
Add
Edit
Delete
OK
Cancel
Help
Device Management
Apply
Reset
Device configuration refreshed successfully.
<admin>
15
1/1/03 1:34:56 AM UTC

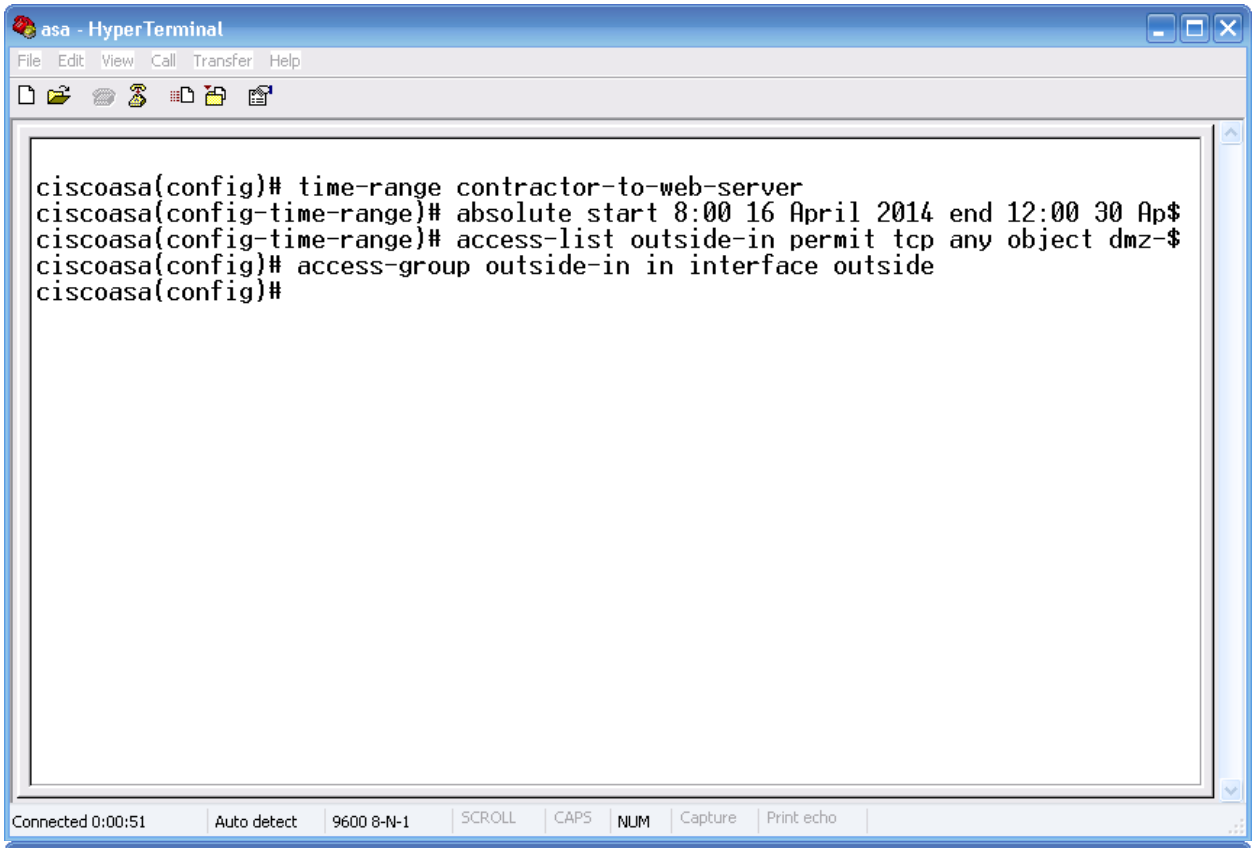

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
cisco
Device List
Firewall
Edit Time Range
Time Range Name: contra
Start Time
Start now
Start at
Month: April
Hour: 00
Recurring Time Ranges
You can further constra
start and stop time spec
Add Recurring Time Range
Specify days of the week and times on which this recurring range will be active
For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only.
Days of the Week
Every day
Weekdays
Weekends
On these days of the week:
Mon Tue Wed Thu Fri Sat Sun
Daily Start Time
Hour 08 Minute 00
Daily End Time (Inclusive)
Hour 12 Minute 00
Specify a weekly interval when this recurring range will be active
For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59.
Weekly Interval
From: Monday Hour: 00 Minute: 00
From: Friday Hour: 23 Minute: 59
OK Cancel Help
Year: 2014
Add
Edit
Delete
Apply Reset
Device Management
Configuration changes saved successfully.
<admin>
15
1/1/03 1:37:16 AM UTC

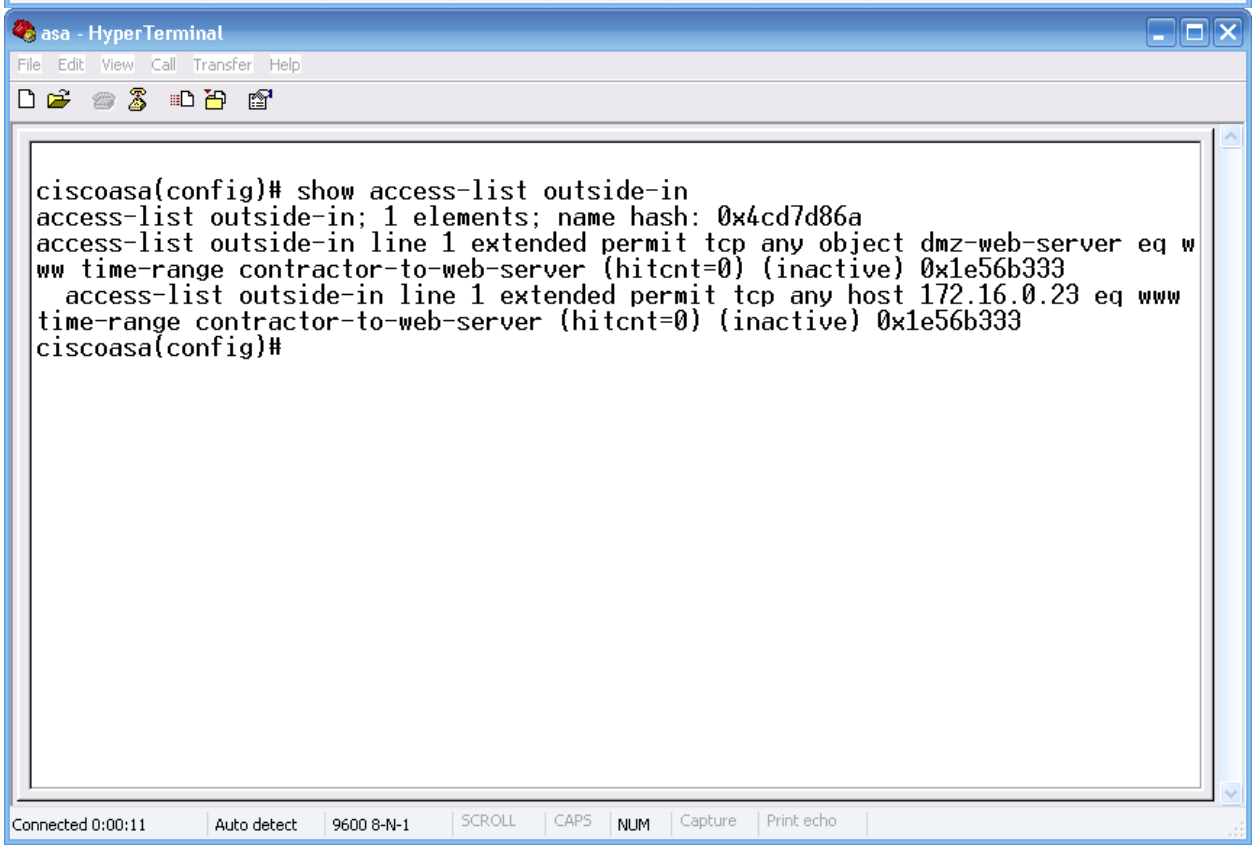

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Configuration > Firewall > Objects > Time Ranges
Edit Time Range
Time Range Name: contractor-to-web-server
Start Time
Start now
Start at
Month: April Day: 16 Year: 2014
Hour: 00 Minute: 00
End Time
Never end
End at (inclusive)
Month: April Day: 30 Year: 2014
Hour: 12 Minute: 00
Recurring Time Ranges
You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.
Monday Wednesday Friday 08:00 through 12:00
Add
Edit
Delete
OK
Cancel
Help
Apply
Reset
Device List
Device Management
Configuration changes saved successfully.
<admin>
15
1/1/03 1:37:36 AM UTC

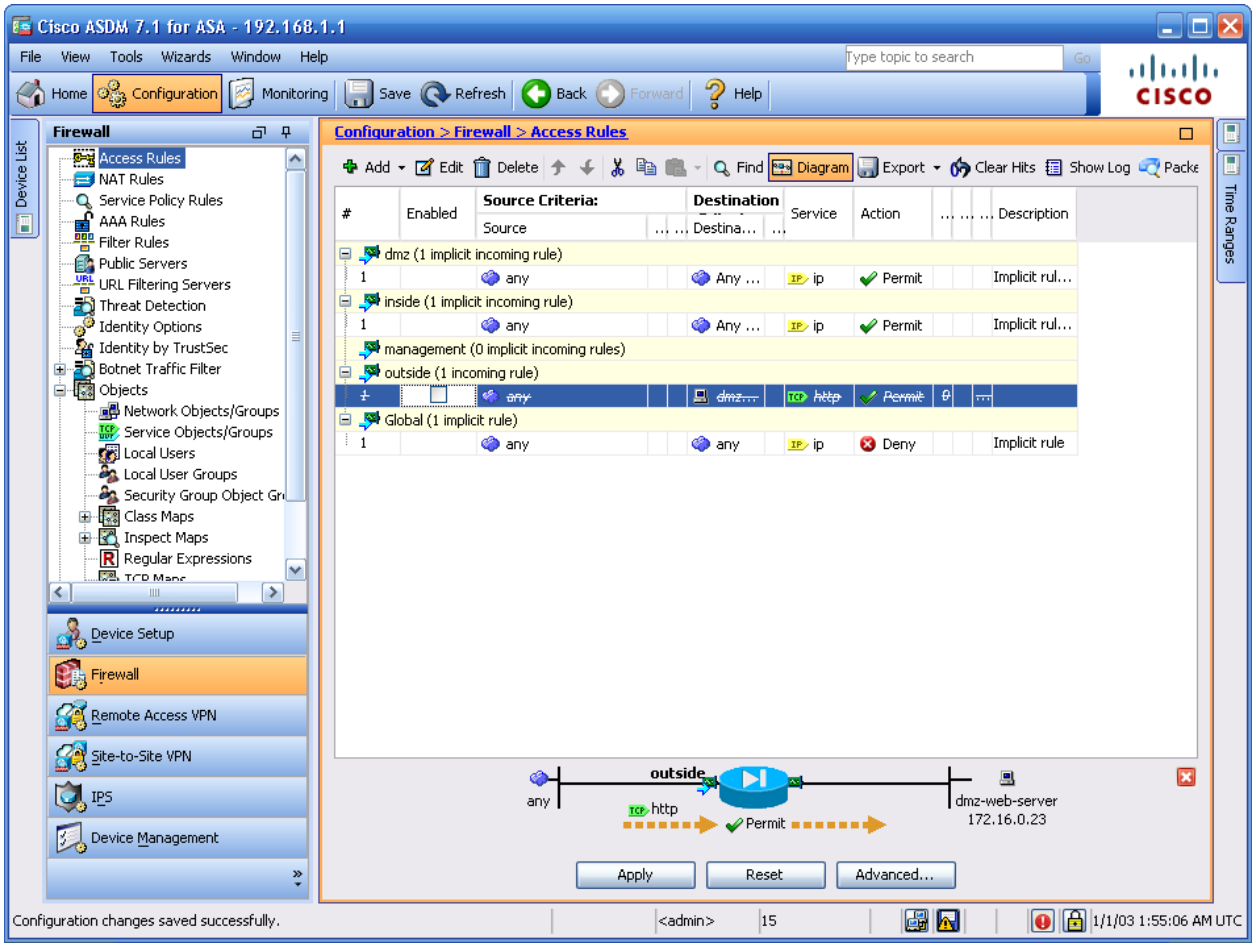

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
cisco
Device List
Firewall
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Gr
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Objects > Time Ranges
Add Edit Delete
Name
Start Time
End Time
Recurring Entries
contractor-to-web-server
00:00 16 April 2014
12:00 30 April 2014
Monday Wednesday Friday 08:00 thr.
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:37:46 AM UTC

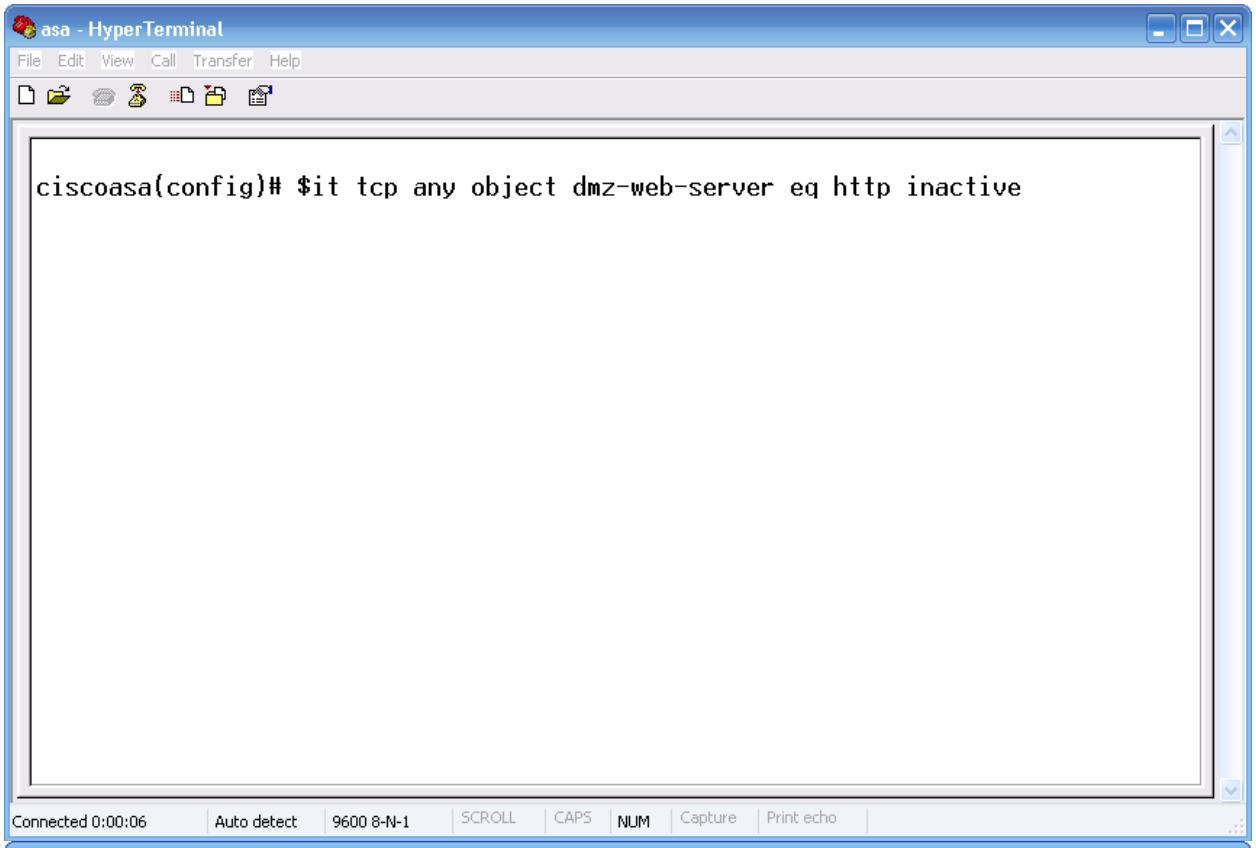

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards
Home Configuratio
Firewall
Access Rules
NAT Rules
Service Policy Rul
AAA Rules
Filter Rules
Public Servers
URL Filtering Serv
Threat Detection
Identity Options
Identity by Trust
Botnet Traffic Filt
Objects
Network Obje
Service Objec
Local Users
Local User Gr
Security Grou
Class Maps
Inspect Maps
Regular Expre
Device Setup
Firewall
Remote Access VPI
Site-to-Site VPN
IPS
Device Managemer
Device List
Time Ranges
Show Log
Packe
Add Access Rule
Interface: outside
Action: Permit Deny
Source Criteria
Source: any
User:
Security Group:
Destination Criteria
Destination: dmz-web-server
Security Group:
Service: tcp/http
Description:
Enable Logging
Logging Level: Default
More Options
Enable Rule
Traffic Direction: In Out
Source Service: (TCP or UDP service only)
Logging Interval: 300 seconds
Time Range: contractor-to-web-server
OK
Cancel
Help
Configuration changes saved successfully.
<admin>
15
1/1/03 1:39:46 AM UTC

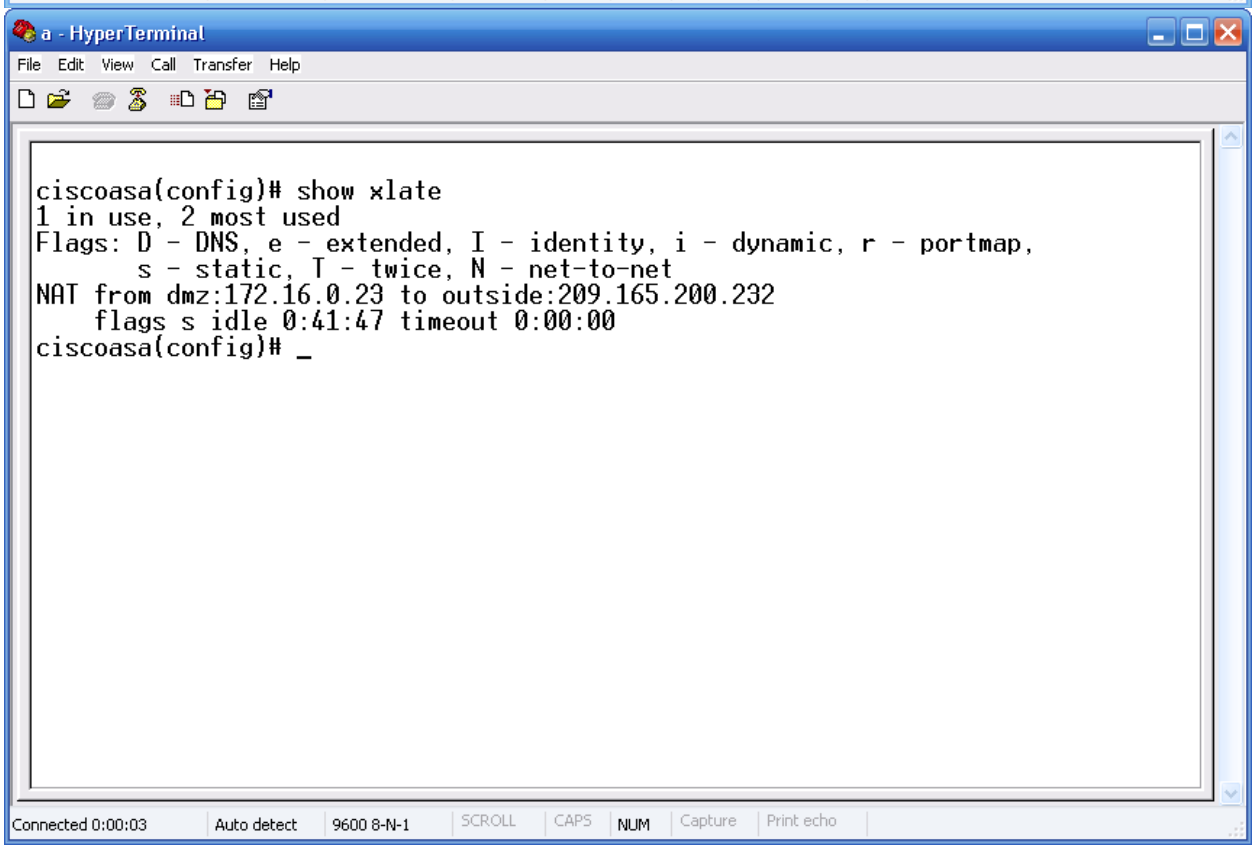

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log
Enabled Source Criteria: Source Destination Service Action Description
dmz (1 implicit incoming rule)
1 any Any ... ip Permit Implicit rul...
inside (1 implicit incoming rule)
1 any Any ... ip Permit Implicit rul...
management (0 implicit incoming rules)
outside (1 incoming rule)
1 any dmz... http Permit
Global (1 implicit rule)
1 any any ip Deny Implicit rule
any
outside
http
Permit
dmz-web-server
172.16.0.23
Apply Reset Advanced...
Time Ranges
Configuration changes saved successfully.
<admin> 15
1/1/03 1:40:16 AM UTC

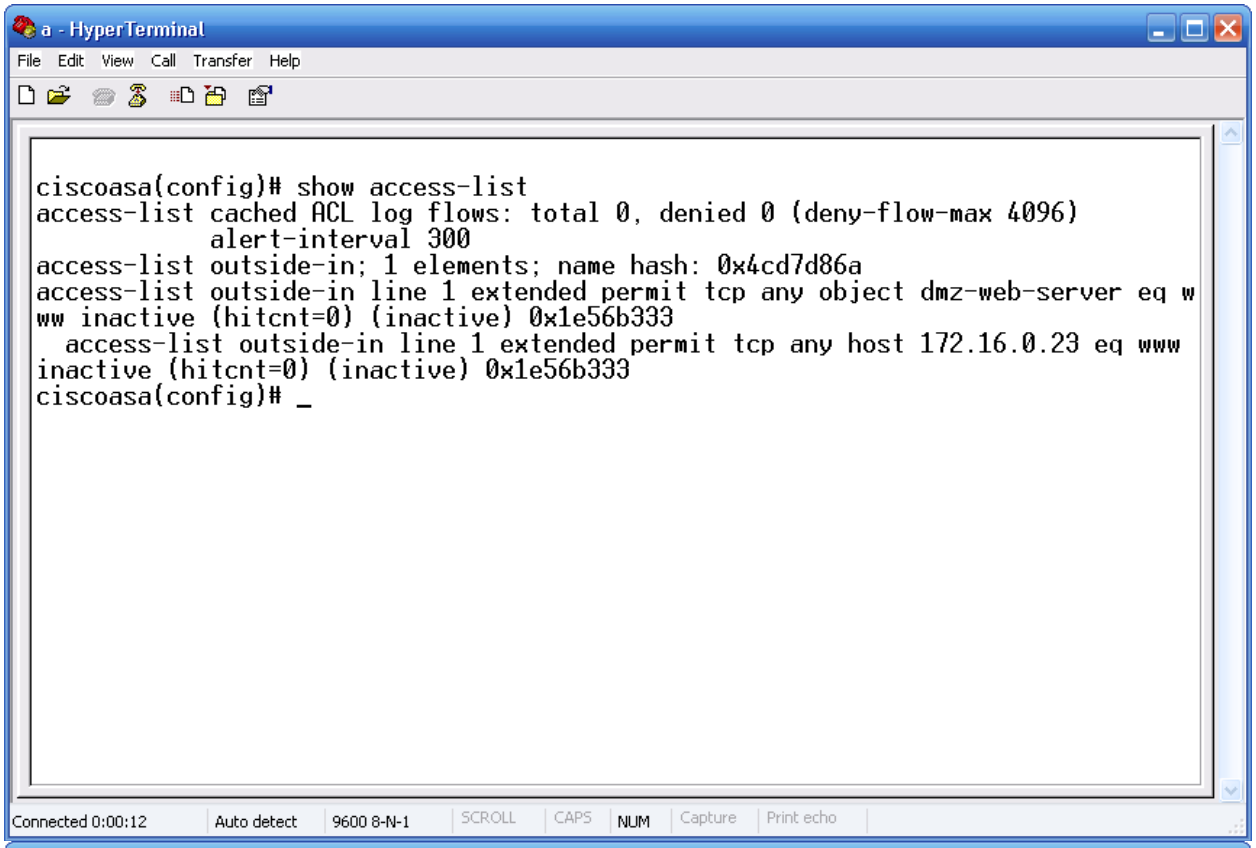

asa - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# time-range contractor-to-web-server
ciscoasa(config-time-range)# absolute start 8:00 16 April 2014 end 12:00 30 Ap$
ciscoasa(config-time-range)# access-list outside-in permit tcp any object dmz-$
ciscoasa(config)# access-group outside-in in interface outside
ciscoasa(config)#
Connected 0:00:51 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

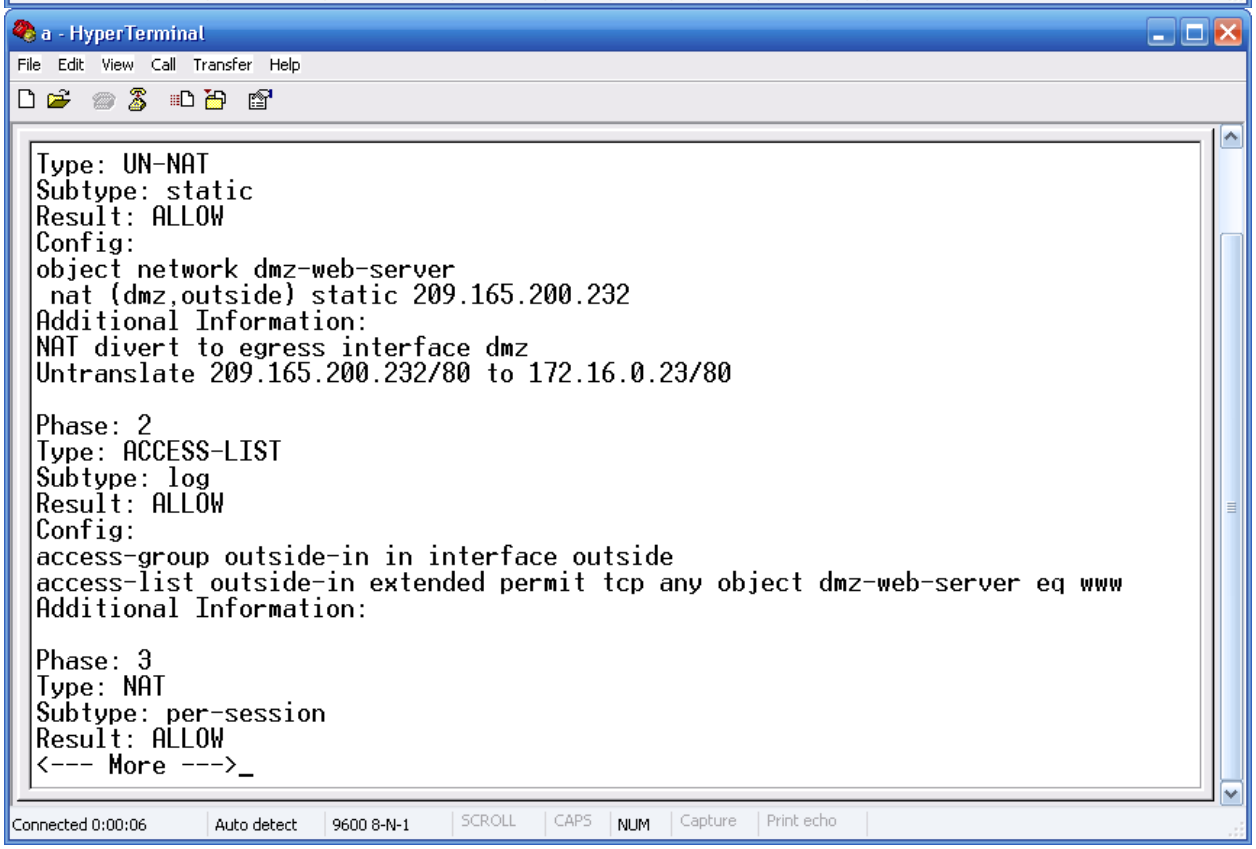

asa - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# show access-list outside-in
access-list outside-in; 1 elements; name hash: 0x4cd7d86a
access-list outside-in line 1 extended permit tcp any object dmz-web-server eq w
ww time-range contractor-to-web-server (hitcnt=0) (inactive) 0x1e56b333
access-list outside-in line 1 extended permit tcp any host 172.16.0.23 eq www
time-range contractor-to-web-server (hitcnt=0) (inactive) 0x1e56b333
ciscoasa(config)#
Connected 0:00:11 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

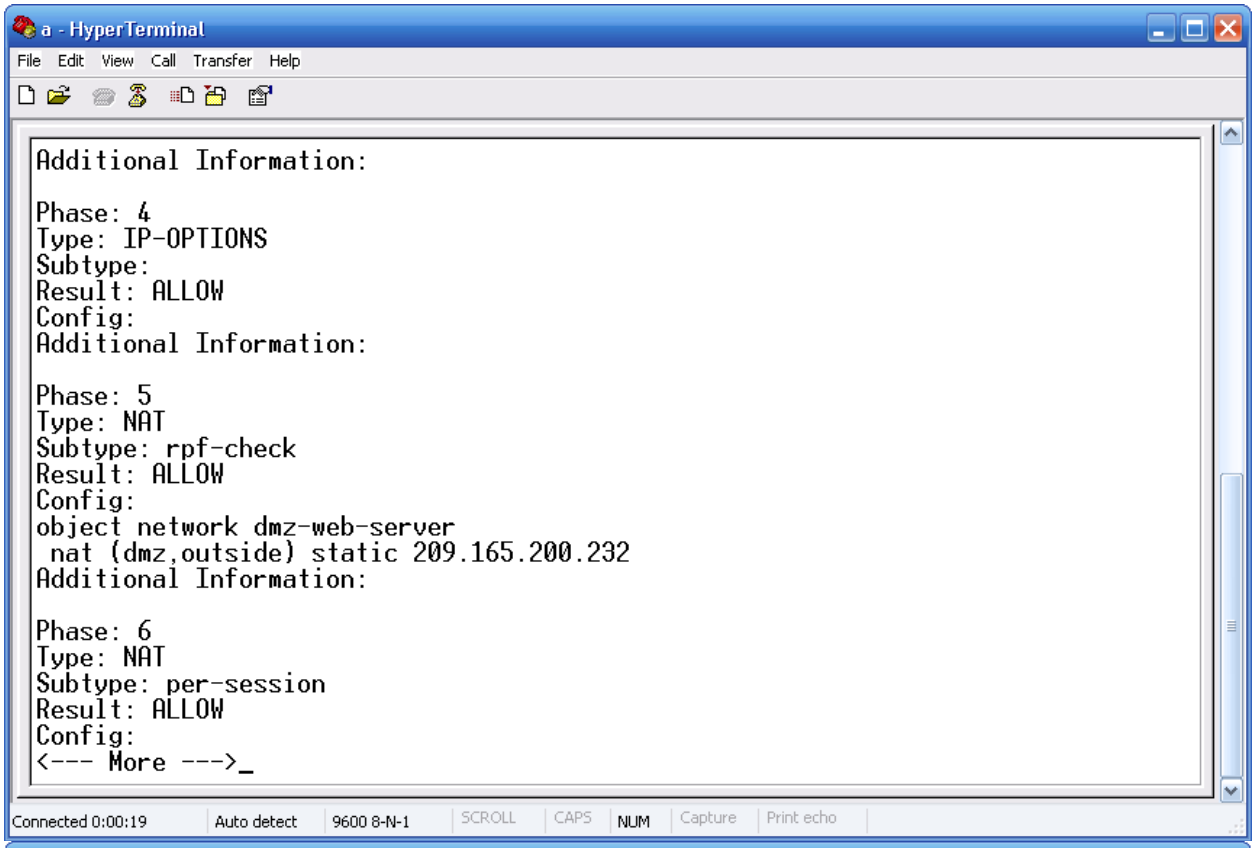

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log
Enabled Source Criteria: Source Destination Service Action Description
dmz (1 implicit incoming rule)
1 any Any ... ip Permit Implicit rul...
inside (1 implicit incoming rule)
1 any Any ... ip Permit Implicit rul...
management (0 implicit incoming rules)
outside (1 incoming rule)
any http Permit
Global (1 implicit rule)
1 any any ip Deny Implicit rule
any
outside
http
Permit
dmz-web-server
172.16.0.23
Apply Reset Advanced...
Configuration changes saved successfully.
<admin> 15
1/1/03 1:55:06 AM UTC

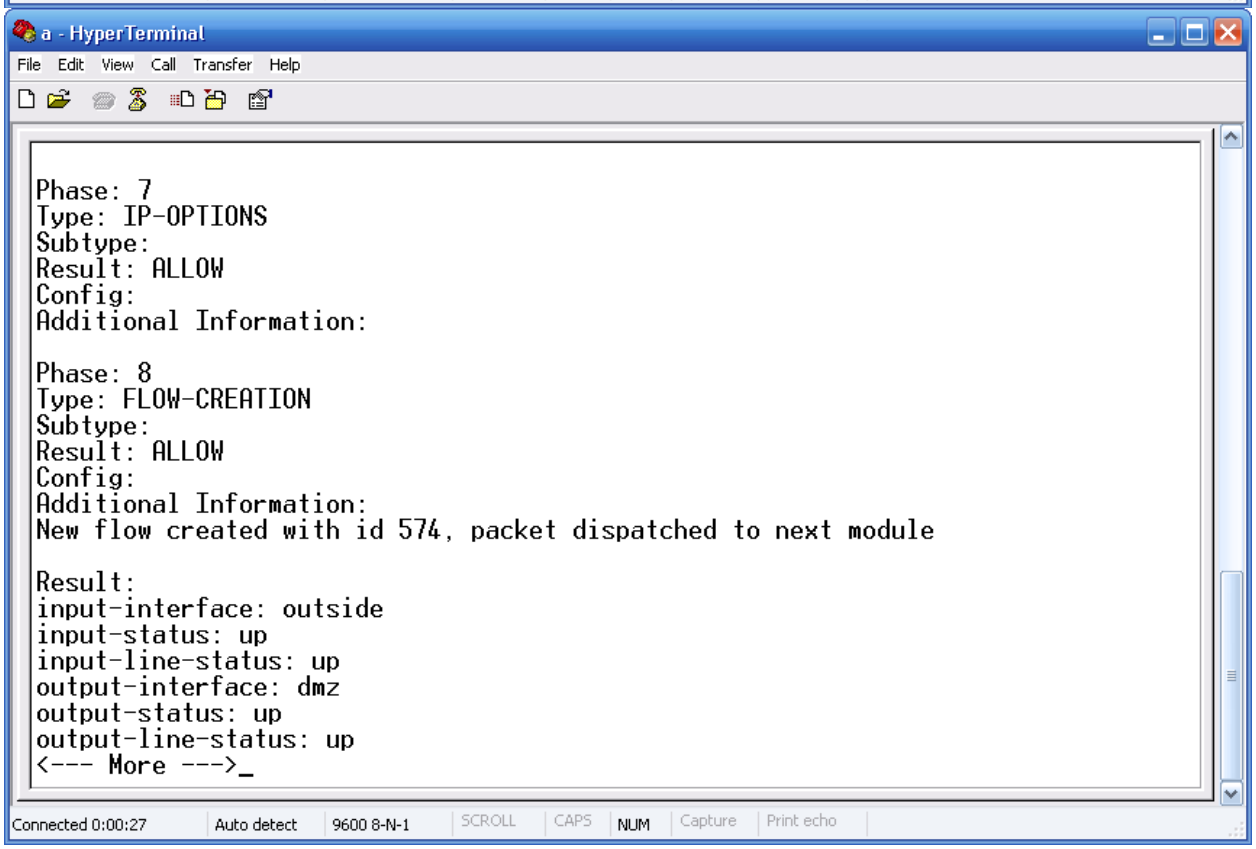

asa - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# $it tcp any object dmz-web-server eq http inactive
Connected 0:00:06 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

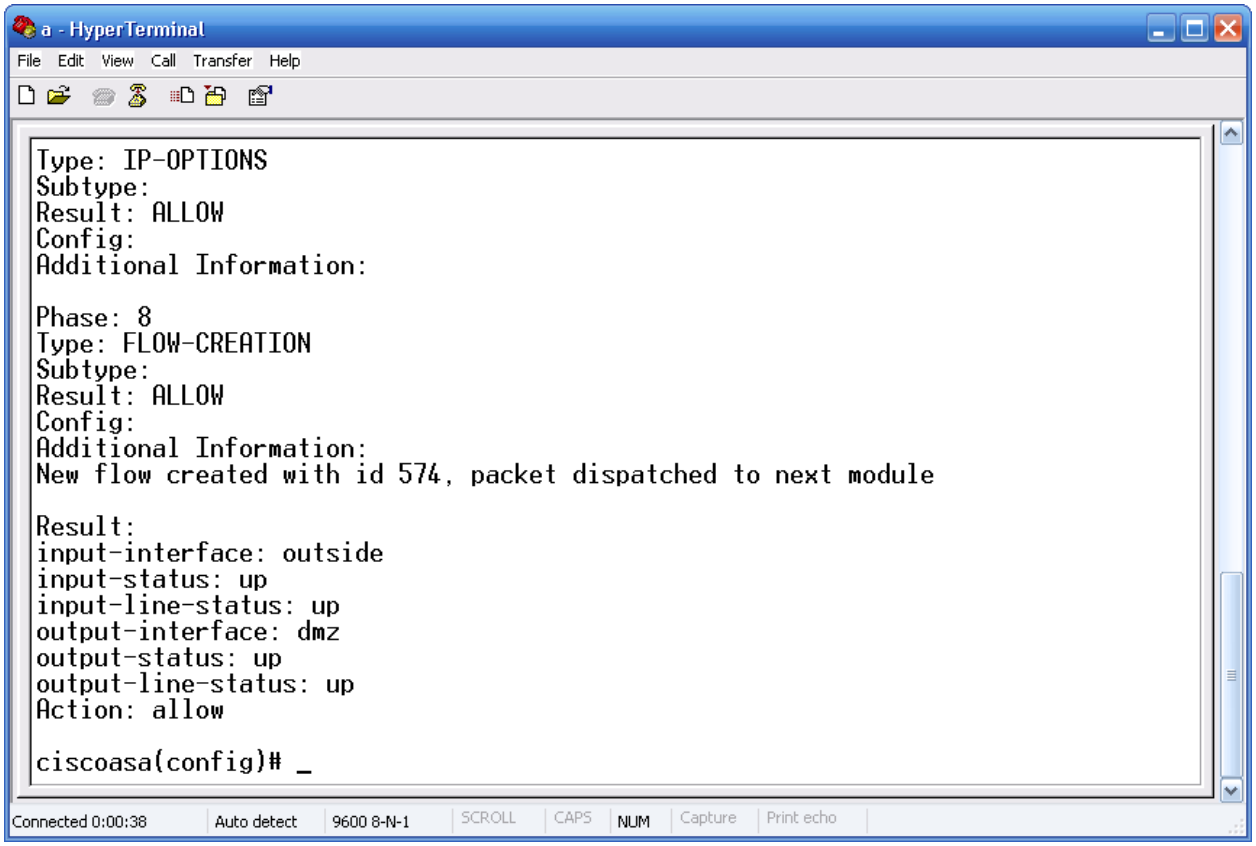

a - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# show xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
NAT from dmz:172.16.0.23 to outside:209.165.200.232
flags s idle 0:41:47 timeout 0:00:00
ciscoasa(config)# _
Connected 0:00:03 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

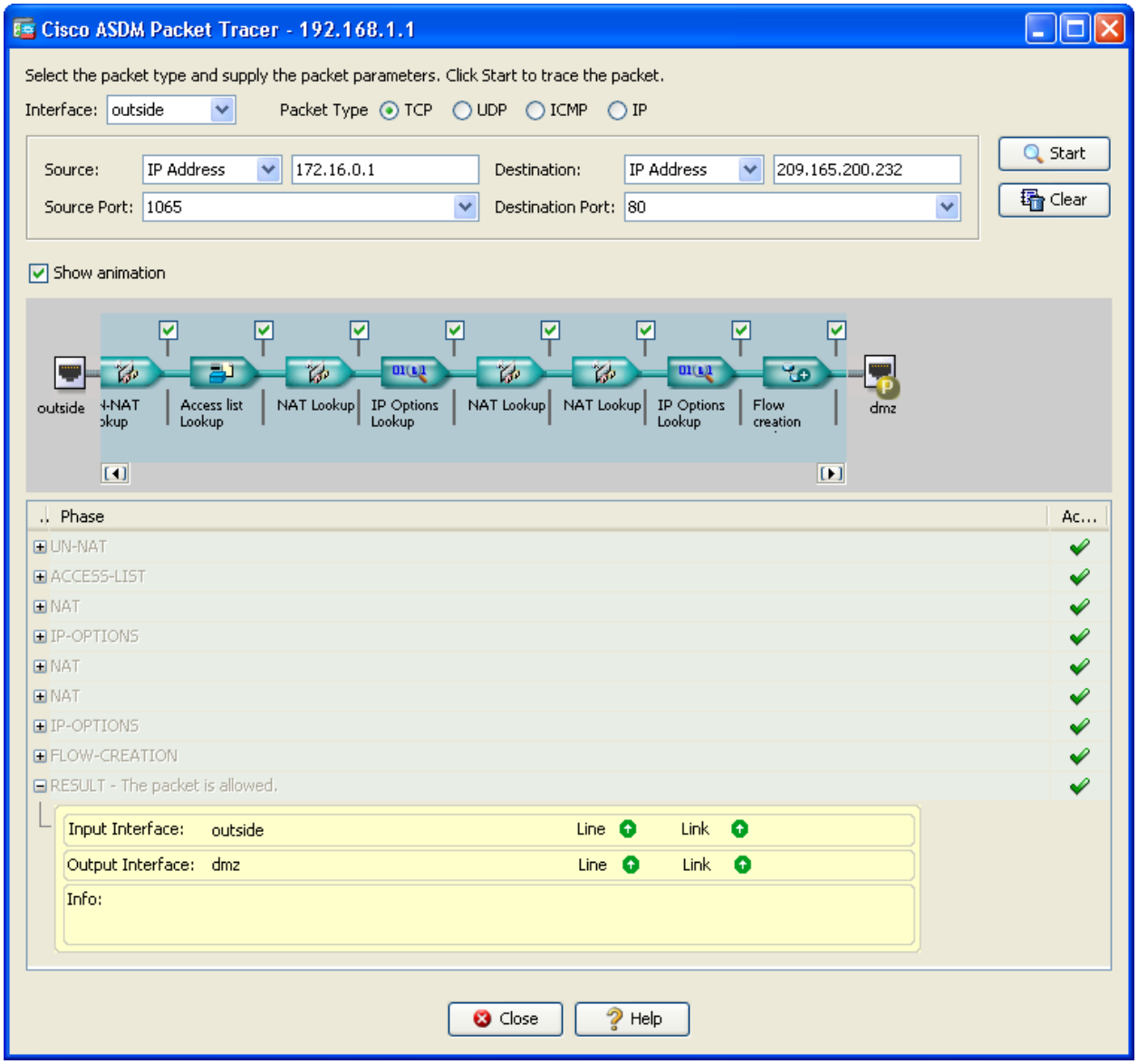

a - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list outside-in; 1 elements; name hash: 0x4cd7d86a
access-list outside-in line 1 extended permit tcp any object dmz-web-server eq w
ww inactive (hitcnt=0) (inactive) 0x1e56b333
access-list outside-in line 1 extended permit tcp any host 172.16.0.23 eq www
inactive (hitcnt=0) (inactive) 0x1e56b333
ciscoasa(config)# _
Connected 0:00:12
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo


a - HyperTerminal
File Edit View Call Transfer Help
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network dmz-web-server
nat (dmz,outside) static 209.165.200.232
Additional Information:
NAT divert to egress interface dmz
Untranslate 209.165.200.232/80 to 172.16.0.23/80
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any object dmz-web-server eq www
Additional Information:
Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
<--- More --->_
Connected 0:00:06
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo


a - HyperTerminal
File Edit View Call Transfer Help
Additional Information:
Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network dmz-web-server
nat (dmz,outside) static 209.165.200.232
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
<--- More --->_
Connected 0:00:19
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo


a - HyperTerminal
File Edit View Call Transfer Help
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 574, packet dispatched to next module
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
<--- More --->_
Connected 0:00:27
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo


a - HyperTerminal
File Edit View Call Transfer Help
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 574, packet dispatched to next module
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
ciscoasa(config)# _
Connected 0:00:38
Auto detect
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo


Cisco ASDM Packet Tracer - 192.168.1.1
Select the packet type and supply the packet parameters. Click Start to trace the packet.
Interface: outside
Packet Type TCP UDP ICMP IP
Source: IP Address 172.16.0.1
Destination: IP Address 209.165.200.232
Source Port: 1065
Destination Port: 80
Start
Clear
Show animation
outside
Access list Lookup
NAT Lookup
IP Options Lookup
NAT Lookup
NAT Lookup
IP Options Lookup
Flow creation
dmz
Phase
Ac...
UN-NAT
ACCESS-LIST
NAT
IP-OPTIONS
NAT
NAT
IP-OPTIONS
FLOW-CREATION
RESULT - The packet is allowed.
Input Interface: outside Line Link
Output Interface: dmz Line Link
Info:
Close
Help