DUMPSBOSS.

CCNP Security Implementing Cisco Secure Mobility Solutions (SIMOS)

Cisco 300-209

Version Demo

Total Demo Questions: 19

Total Premium Questions: 405

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

What are two features of Cisco GET VPN? (Choose two.)

A. allows for optimal routing

B. uses public Internet

C. provides encryption for MPLS

D. provides point-to-point IPsec SA

E. uses MGRE

ANSWER: A C

QUESTION NO: 2

Refer to the exhibit.

You are configuring a laptop with the Cisco VPN Client, which uses digital certificates for authentication.

Which protocol does the Cisco VPN Client use to retrieve the digital certificate from the CA server?

A. FTP

B. LDAP

C. HTTPS

D. SCEP

E. OCSP

ANSWER: D

Explanation:

About CRLs

Certificate Revocation Lists provide the security appliance with one means of determining whether a certificate that is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of the configuration of a trustpoint.

You can configure the security appliance to make CRL checks mandatory when authenticating a certificate (revocation-check crl command). You can also make the CRL check optional by adding the none argument (revocation-check crl none command), which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a length of time configurable for each trustpoint. When the security appliance has cached a CRL for more than the length of time it is configured to cache CRLs, the security appliance considers the CRL too old to be reliable, or "stale". The security appliance attempts to retrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL. Reference: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

QUESTION NO: 3

A custom desktop application needs to access an internal server. An administrator is tasked with configuring the company's SSL VPN gateway to allow remote users to work. Which two technologies would accommodate the company's requirement? (Choose two).

A. AnyConnect client

B. Smart Tunnels

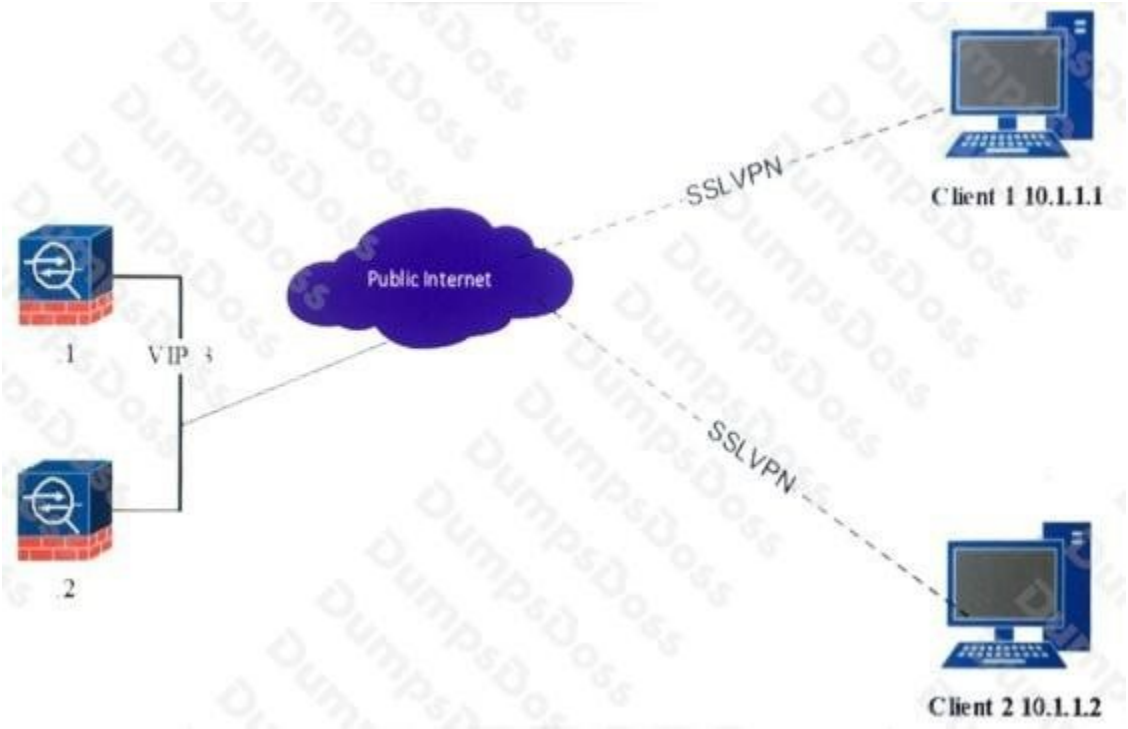
C. Email Proxy

D. Content Rewriter

E. Portal Customizations

ANSWER: A B

QUESTION NO: 4



Refer to the exhibit. VPN load balancing provides a way to distribute remote access, IPsec, and SSL VPN connections across multiple security appliances. Which remote access client types does the load balancing feature support?

A. IPsec site-to-site tunnels

B. L2TP over IPsec

C. OpenVPN

D. Cisco AnyConnect Secure Mobility Client

ANSWER: D

QUESTION NO: 5

Which two troubleshooting steps should be taken when Cisco AnyConnect cannot establish an IKEv2 connection, while SSL works fine? (Choose two.)

A. Verify that the primary protocol on the client machine is set to IPsec.

B. Verify that AnyConnect is enabled on the correct interface.

C. Verify that the IKEv2 protocol is enabled on the group policy.

D. Verify that ASDM and AnyConnect are not using the same port.

E. Verify that SSL and IKEv2 certificates are not referencing the same trustpoint.

ANSWER: A C

QUESTION NO: 6

An IOS SSL VPN is configured to forward TCP ports. A remote user cannot access the corporate FTP site with a Web browser. What is a possible reason for the failure?

A. The user's FTP application is not supported.

B. The user is connecting to an IOS VPN gateway configured in Thin Client Mode.

C. The user is connecting to an IOS VPN gateway configured in Tunnel Mode.

D. The user's operating system is not supported.

ANSWER: B

Explanation:

Thin-Client SSL VPN (Port Forwarding)

A remote client must download a small, Java-based applet for secure access of TCP applications that use static port numbers. UDP is not supported. Examples include access to POP3, SMTP, IMAP, SSH, and Telnet. The user needs local administrative privileges because changes are made to files on the local machine. This method of SSL VPN does not work with applications that use dynamic port assignments, for example, several FTP applications.

Reference:

http://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70664-IOSthinclient.html

QUESTION NO: 7

Which three types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose three.)

A. SAML

B. HTTP POST

C. HTTP Basic

D. NTLM

E. Kerberos

F. OAuth 2.0

ANSWER: B C D

QUESTION NO: 8

Which two examples of transform sets are contained in the IKEv2 default proposal? (Choose two.)

A. aes-cbc-192, sha256, 14

B. 3des, md5, 5

C. 3des, sha1, 1

D. aes-cbc-128, sha, 5

ANSWER: B D

QUESTION NO: 9

A company has a Flex VPN solution for remote access and one of their Cisco any Connect remote clients is having trouble connecting properly.

Which command verifies that packets are being encrypted and decrypted?

A. show crypto session active

B. show crypto ikev2 stats

C. show crypto ikev1 sa

D. show crypto ikev2 sa

E. show crypto session detail

ANSWER: E

QUESTION NO: 10

An engineer is configuring high availability for crypto-map-based site-to-site VPNs on Cisco IOS devices. Which protocol must be used?

A. VRRP

B. BFD

C. ESP

D. HSRP

ANSWER: D

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/17826-ipsec-feat.html

QUESTION NO: 11

Which three actions can be applied to a traffic class within a type inspect policy map? (Choose three.)

A. drop

B. priority

C. log

D. pass

E. inspect

F. reset

ANSWER: A C F

QUESTION NO: 12

Which option is the main difference between GET VPN and DMVPN?

A. AES encryption support

B. dynamic spoke-to-spoke tunnel communications

C. Next Hop Resolution Protocol

D. Group Domain of Interpretation protocol

ANSWER: B

QUESTION NO: 13

Which are two main use cases for Clientless SSL VPN? (Choose two.)

A. In kiosks that are part of a shared environment

B. When the users do not have admin rights to install a new VPN client

C. When full tunneling is needed to support applications that use TCP, UDP, and ICMP

D. To create VPN site-to-site tunnels in combination with remote access

ANSWER: A B

QUESTION NO: 14

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=#
```

Refer to the exhibit. An engineer encounters a debug message. Which action can the engineer take to eliminate this error message?

A. Use stronger encryption suite.

B. Correct the VPN peer address.

C. Make adjustment to IPSec replay window.

D. Change the preshared key to match.

ANSWER: C

QUESTION NO: 15

In which situation would you enable the Smart Tunnel option with clientless SSL VPN?

A. when a user is using an outdated version of a web browser

B. when an application is failing in the rewrite process

C. when IPsec should be used over SSL VPN

D. when a user has a nonsupported Java version installed

E. when cookies are disabled

ANSWER: B

QUESTION NO: 16

What are the three primary components of a GET VPN network? (Choose three.)

A. Group Domain of Interpretation protocol

B. Simple Network Management Protocol

C. server load balancer

D. accounting server

E. group member

F. key server

ANSWER: A E F

QUESTION NO: 17 - (SIMULATION)

SIMULATION

Scenario

You are the network security administrator for your organization. Your company is growing and a remote branch office is being created. You are tasked with configuring your headquarters Cisco ASA to create a site-to-site IPsec VPN connection to the branch office Cisco ISR. The branch office ISR has already been deployed and configured and you need to complete the IPsec connectivity configurations on the HQ ASA to bring the new office online.

Use the following parameters to complete your configuration using ASDM. For this exercise, not all ASDM screens are active.

▪ Enable IKEv1 on outside I/F for Site-to-site VPN ▪ Add a Connection Profile with the following parameters: - Peer IP: 203.0.113.1

- Connection name: 203.0.113.1

- Local protected network: 10.10.9.0/24

- Remote protected network: 10.11.11.0/24

- Group Policy Name: use the default policy name supplied

- Preshared key: cisco

- Disable IKEv2

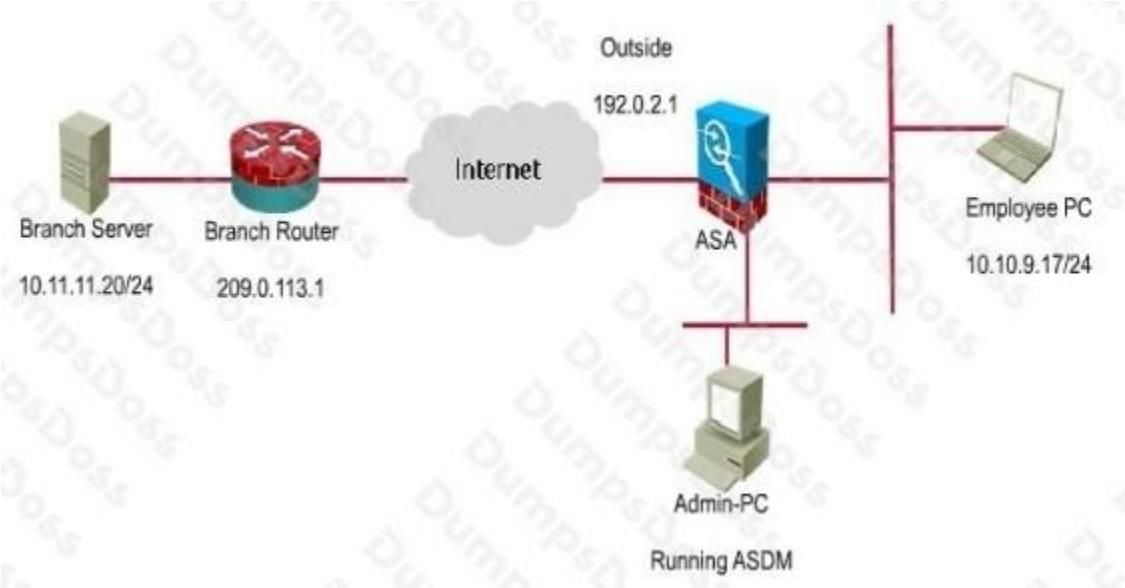
- Encryption Algorithms: use the ASA defaults

▪ Disable pre-configured NAT for testing of the IPsec tunnel - Disable the outside NAT pool rule

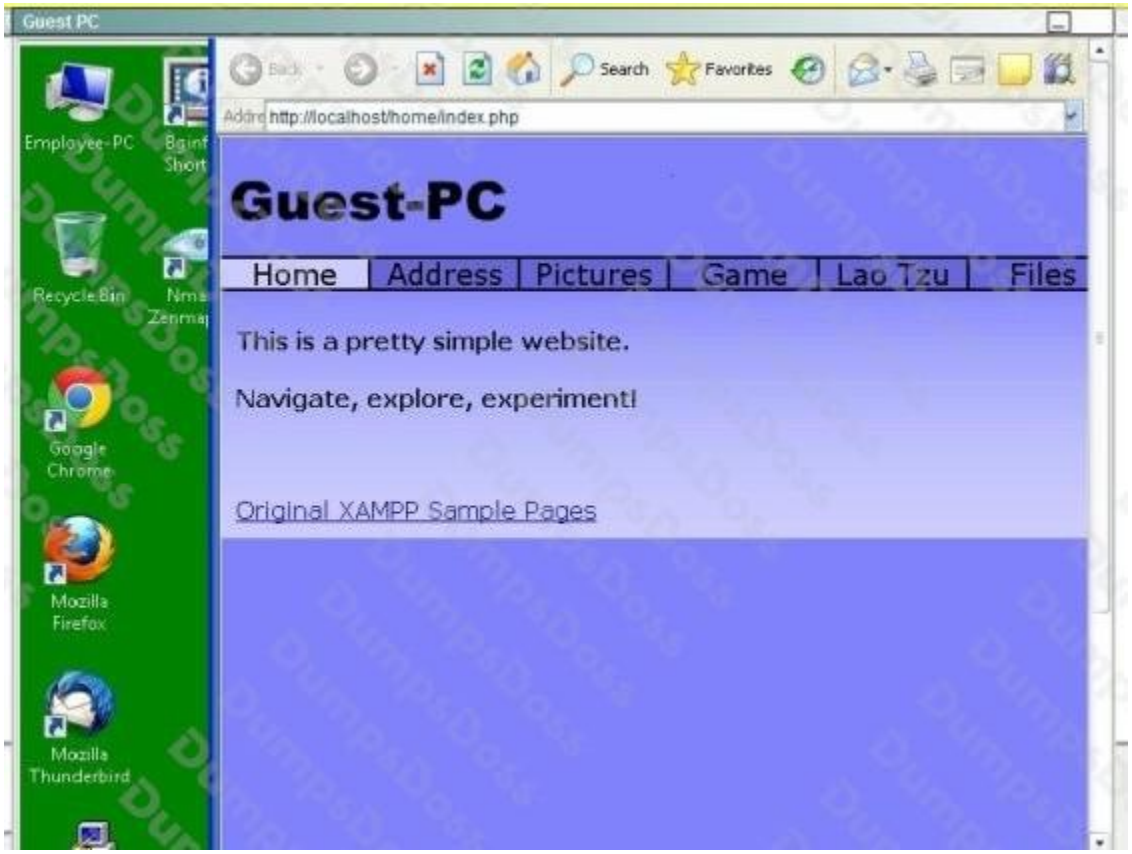
▪ Establish the IPsec tunnel by sending ICMP pings from the Employee PC to the Branch Server at IP address 10.11.11.20
▪ Verify tunnel establishment in ASDM VPN Statistics> Sessions window pane

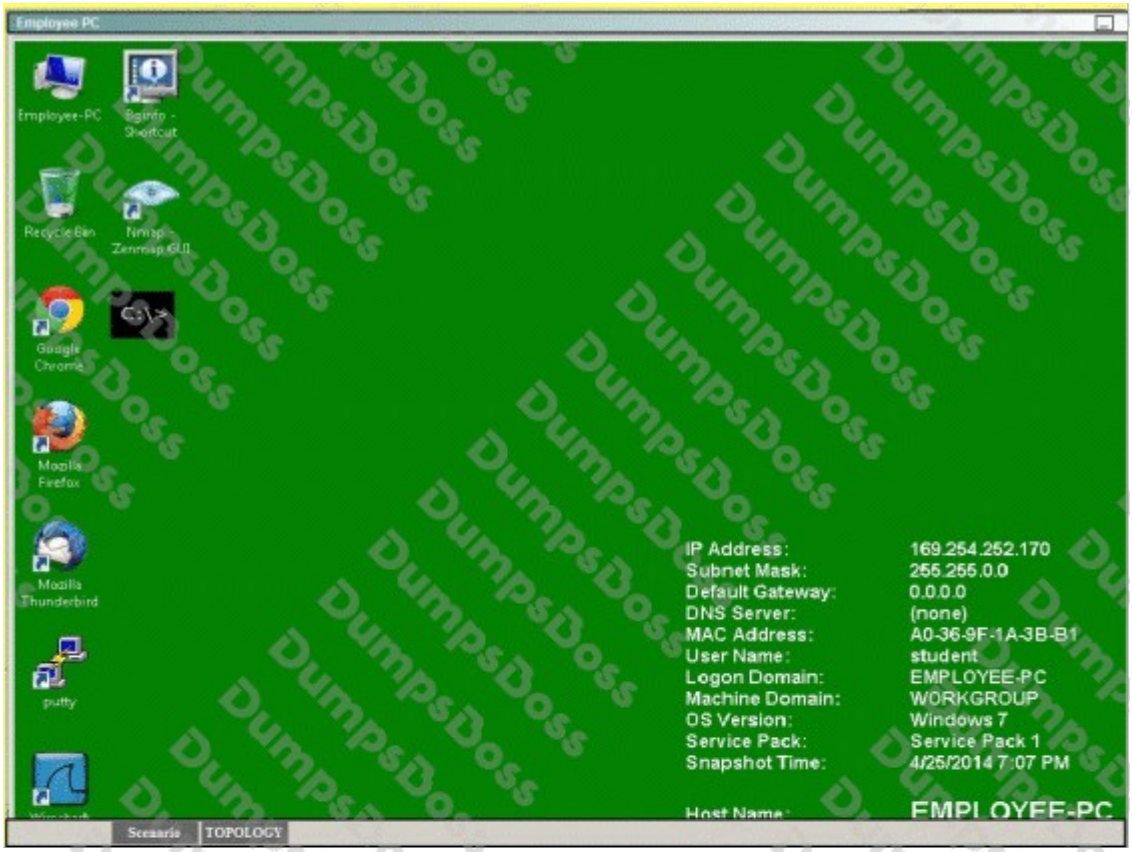
You have completed this exercise when you have successfully configured, established, and verified site-to-site IPsec connectivity between the ASA and the Branch ISR.

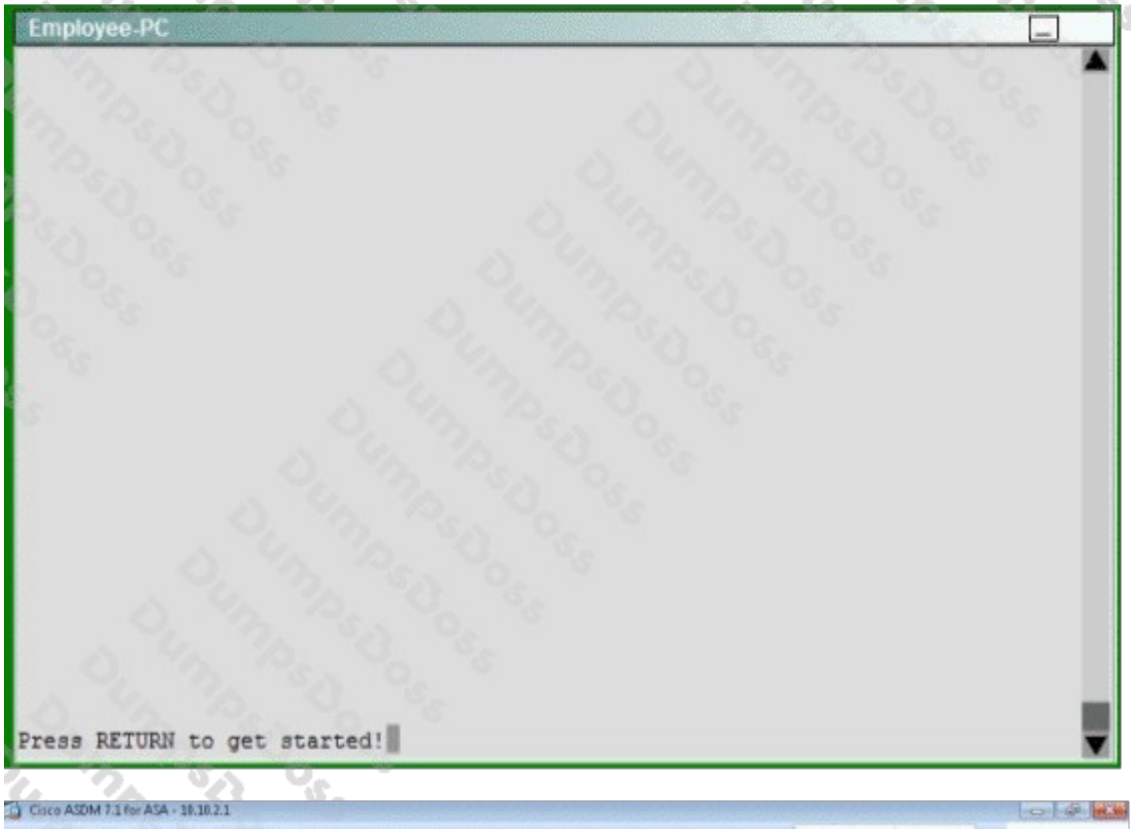
Topology

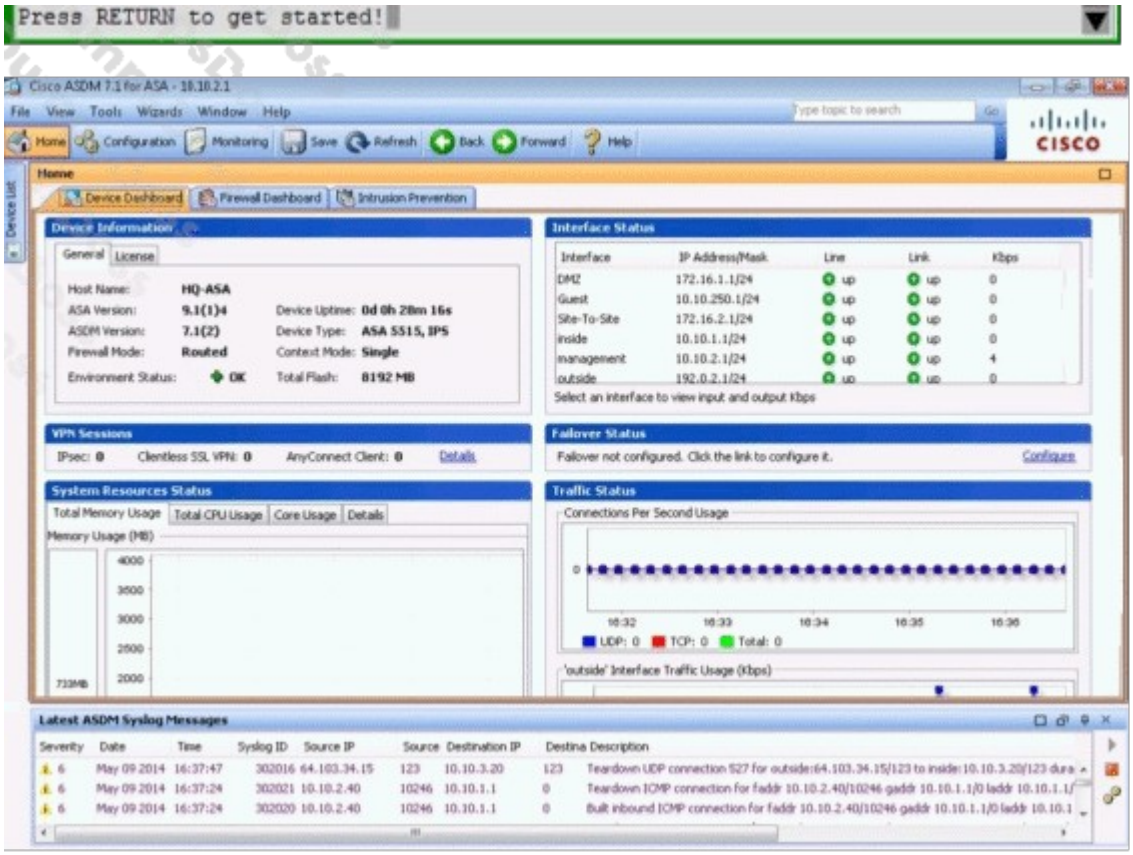

Outside
192.0.2.1
Internet
Branch Server
10.11.11.20/24
Branch Router
209.0.113.1
ASA
Employee PC
10.10.9.17/24
Admin-PC
Running ASDM

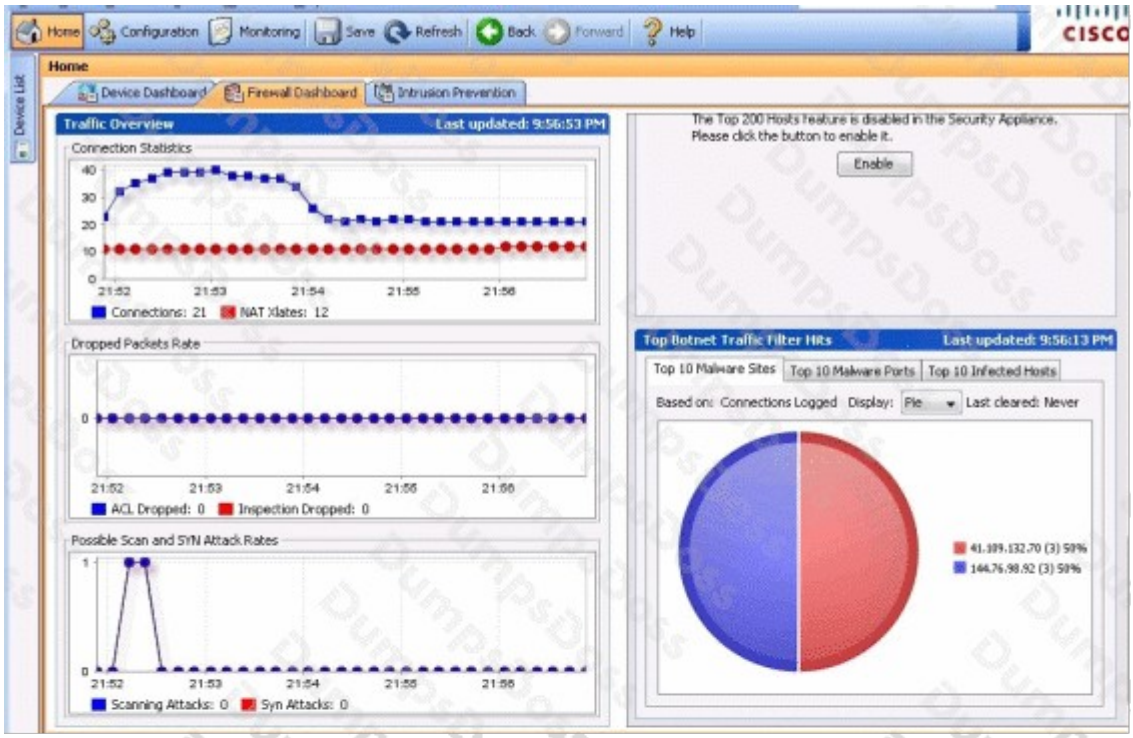

Guest PC
Employee-PC
Recycle Bin
Google Chrome
Mozilla Firefox
Mozilla Thunderbird
IP Address:
Subnet Mask:
Default Gateway
DNS Server:
MAC Address:
Scenario
TOPOLOGY

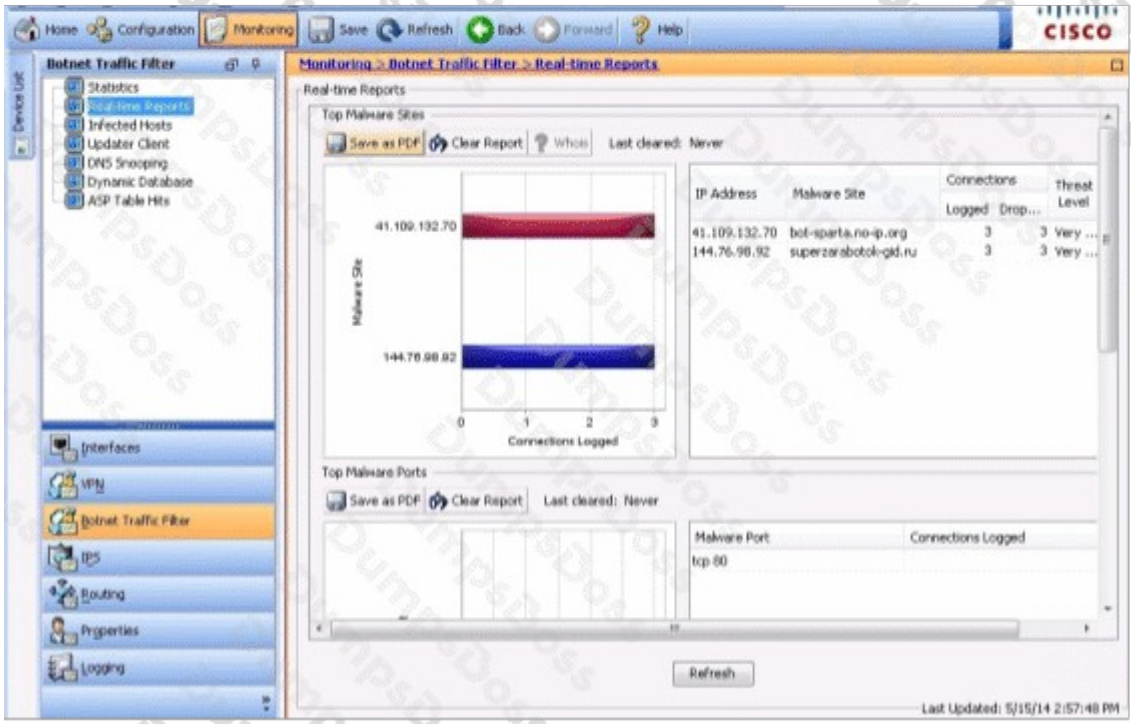

Guest PC
Employee-PC
Recycle Bin
Google Chrome
Mozilla Firefox
Mozilla Thunderbird
Search
Favorites
http://localhost/home/index.php
Guest-PC
Home
Address
Pictures
Game
Lao Tzu
Files
This is a pretty simple website.
Navigate, explore, experiment!
Original XAMPP Sample Pages

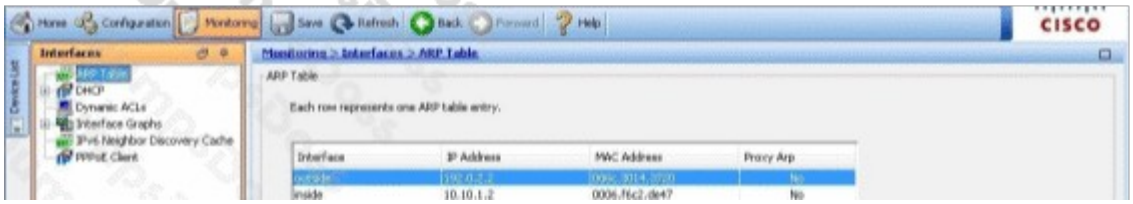

Employee PC
Employee-PC
Recycle Bin
Google Chrome
Mozilla Firefox
Mozilla Thunderbird
putty
IP Address: 169.254.252.170
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
DNS Server: (none)
MAC Address: A0-36-9F-1A-3B-B1
User Name: student
Logon Domain: EMPLOYEE-PC
Machine Domain: WORKGROUP
OS Version: Windows 7
Service Pack: Service Pack 1
Snapshot Time: 4/25/2014 7:07 PM
Host Name: EMPLOYEE-PC
Scenario
TOPOLOGY

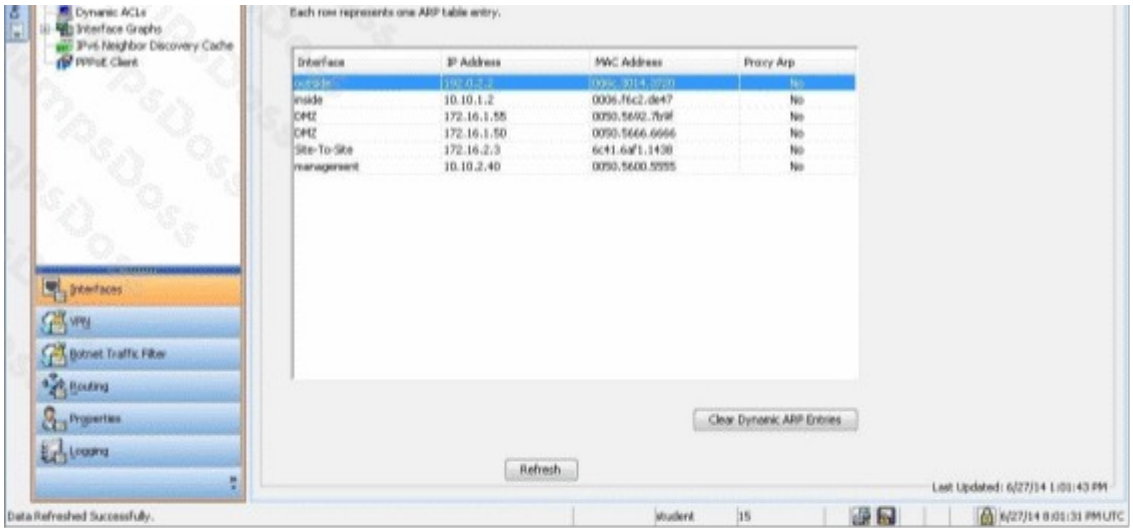

Employee-PC
Press RETURN to get started!
Cisco ASDM 7.1 for ASA - 10.10.2.1

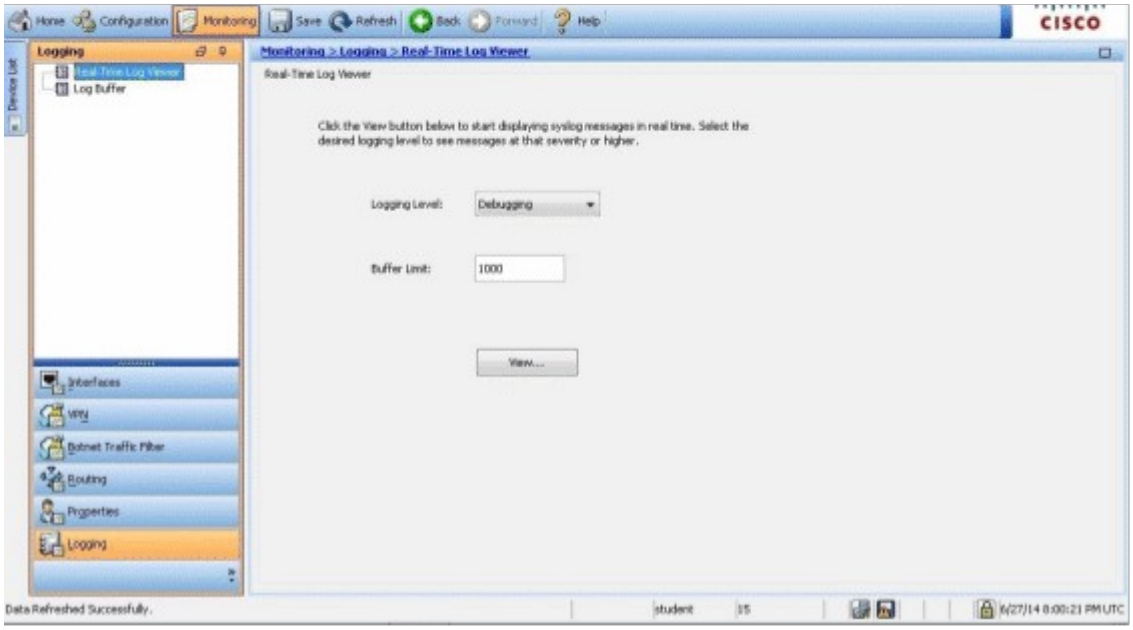

Press RETURN to get started!
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard Firewall Dashboard Intrusion Prevention
Device Information
General License
Host Name: HQ-ASA
ASA Version: 9.1(1)4 Device Uptime: 0d 0h 28m 16s
ASDM Version: 7.1(2) Device Type: ASA 5515, IPS
Firewall Mode: Routed Context Mode: Single
Environment Status: OK Total Flash: 8192 MB
Interface Status
Interface IP Address/Mask Line Link Kbps
DMZ 172.16.1.1/24 up up 0
Guest 10.10.250.1/24 up up 0
Site-To-Site 172.16.2.1/24 up up 0
inside 10.10.1.1/24 up up 0
management 10.10.2.1/24 up up 4
outside 192.0.2.1/24 up up 0
Select an interface to view input and output Kbps
VPN Sessions
IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details
Failover Status
Failover not configured. Click the link to configure it. Configure
System Resources Status
Total Memory Usage Total CPU Usage Core Usage Details
Memory Usage (MB)
4000
3500
3000
2500
2000
733MB
Traffic Status
Connections Per Second Usage
0
16:32 16:33 16:34 16:35 16:36
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Latest ASDM Syslog Messages
Severity Date Time Syslog ID Source IP Source Destination IP Destina Description
6 May 09 2014 16:37:47 302016 64.103.34.15 123 10.10.3.20 123 Teardown UDP connection 527 for outside:64.103.34.15/123 to inside:10.10.3.20/123 dura
6 May 09 2014 16:37:24 302021 10.10.2.40 10246 10.10.1.1 0 Teardown ICMP connection for faddr 10.10.2.40/10246 gaddr 10.10.1.1/0 laddr 10.10.1.1/
6 May 09 2014 16:37:24 302020 10.10.2.40 10246 10.10.1.1 0 Built inbound ICMP connection for faddr 10.10.2.40/10246 gaddr 10.10.1.1/0 laddr 10.10.1

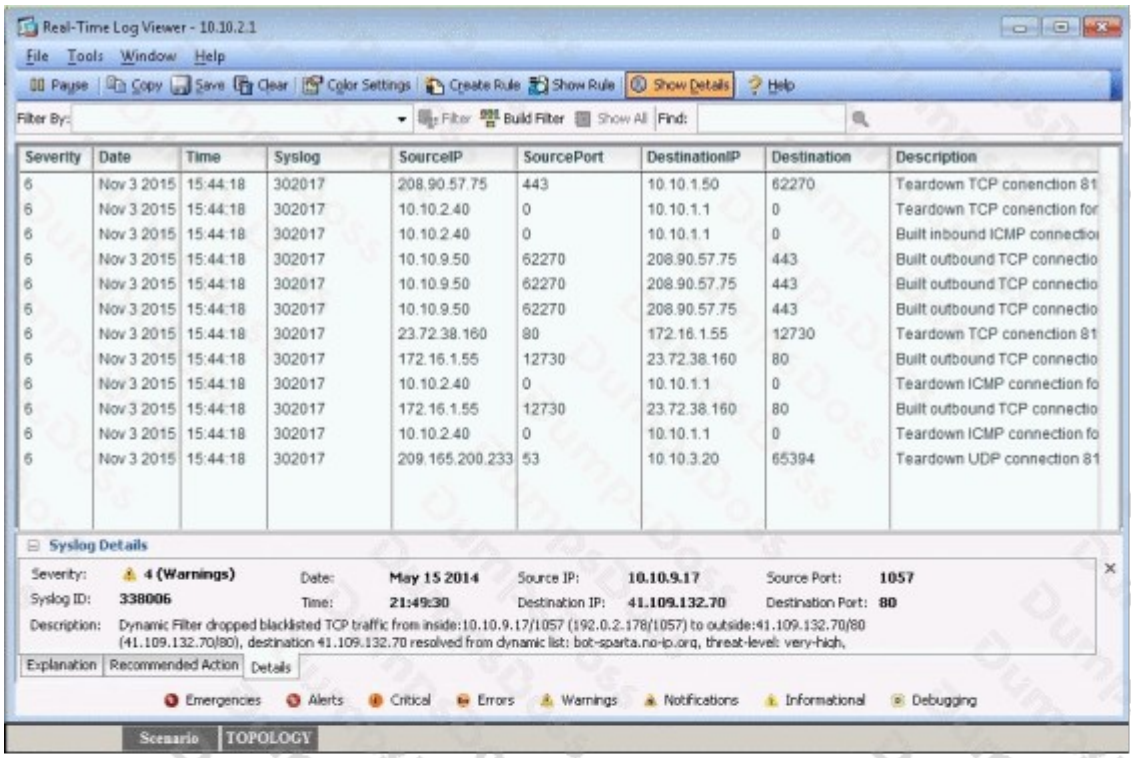

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Device Dashboard
Firewall Dashboard
Intrusion Prevention
Traffic Overview
Last updated: 9:56:53 PM
Connection Statistics
Connections: 21
NAT Xlates: 12
The Top 200 Hosts feature is disabled in the Security Appliance.
Please click the button to enable it.
Enable
Dropped Packets Rate
ACL Dropped: 0
Inspection Dropped: 0
Possible Scan and SYN Attack Rates
Scanning Attacks: 0
Syn Attacks: 0
Top Botnet Traffic Filter Hits
Last updated: 9:56:13 PM
Top 10 Malware Sites
Top 10 Malware Ports
Top 10 Infected Hosts
Based on: Connections Logged
Display:
Pie
Last cleared: Never
41.109.132.70 (3) 50%
144.76.98.92 (3) 50%

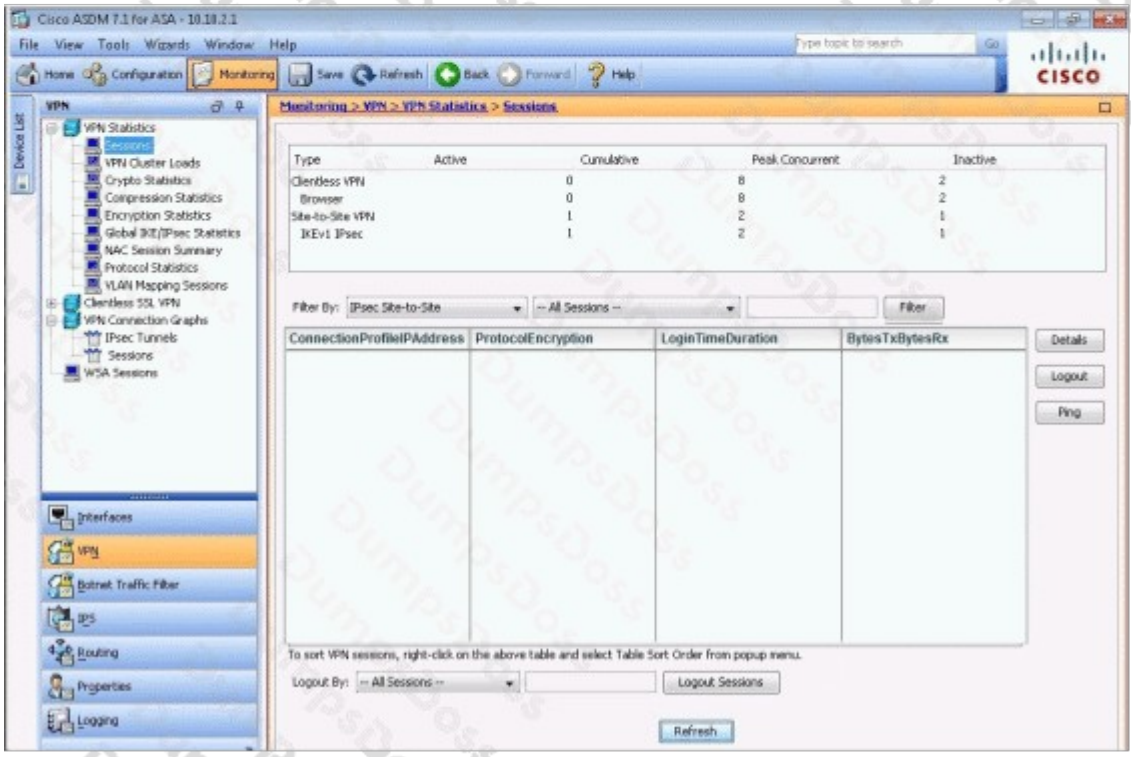

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Botnet Traffic Filter
Statistics
Real-time Reports
Infected Hosts
Updater Client
DNS Snooping
Dynamic Database
ASP Table Hits
Interfaces
VPN
Botnet Traffic Filter
IPS
Routing
Properties
Logging
Monitoring > Botnet Traffic Filter > Real-time Reports
Real-time Reports
Top Malware Sites
Save as PDF
Clear Report
Last cleared: Never
41.109.132.70
144.76.98.92
Malware Site
Connections Logged
IP Address
Malware Site
Connections
Logged
Drop...
Threat Level
41.109.132.70 bot-sparta.no-ip.org 3 3 Very ...
144.76.98.92 superzarabotok-gid.ru 3 3 Very ...
Top Malware Ports
Save as PDF
Clear Report
Last cleared: Never
Malware Port
Connections Logged
tcp 80
Refresh
Last Updated: 5/15/14 2:57:48 PM


Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents one ARP table entry.
Interface
IP Address
MAC Address
Proxy Arp
inside
10.10.1.2
0006.f6c2.de47
No

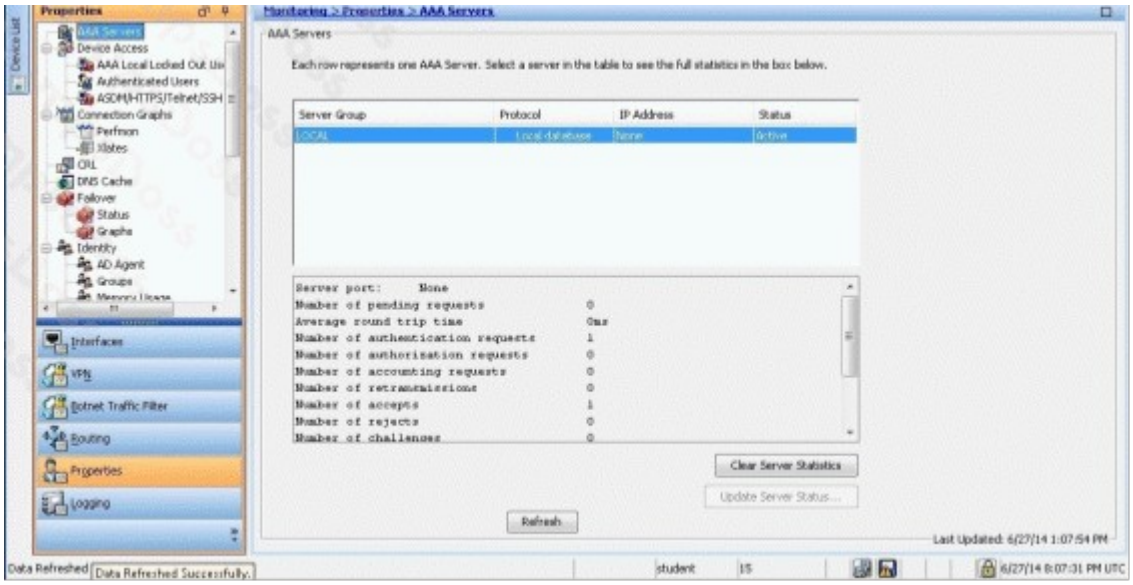

Each row represents one ARP table entry.
Interface
IP Address
MAC Address
Proxy Arp
inside
10.10.1.2
0006.f6c2.de47
No
DMZ
172.16.1.55
0050.5692.7b9f
No
DMZ
172.16.1.50
0050.5666.6666
No
Site-To-Site
172.16.2.3
6c41.6af1.1438
No
management
10.10.2.40
0050.5600.5555
No
Clear Dynamic ARP Entries
Refresh
Last Updated: 6/27/14 1:01:43 PM
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Data Refreshed Successfully.
student
15

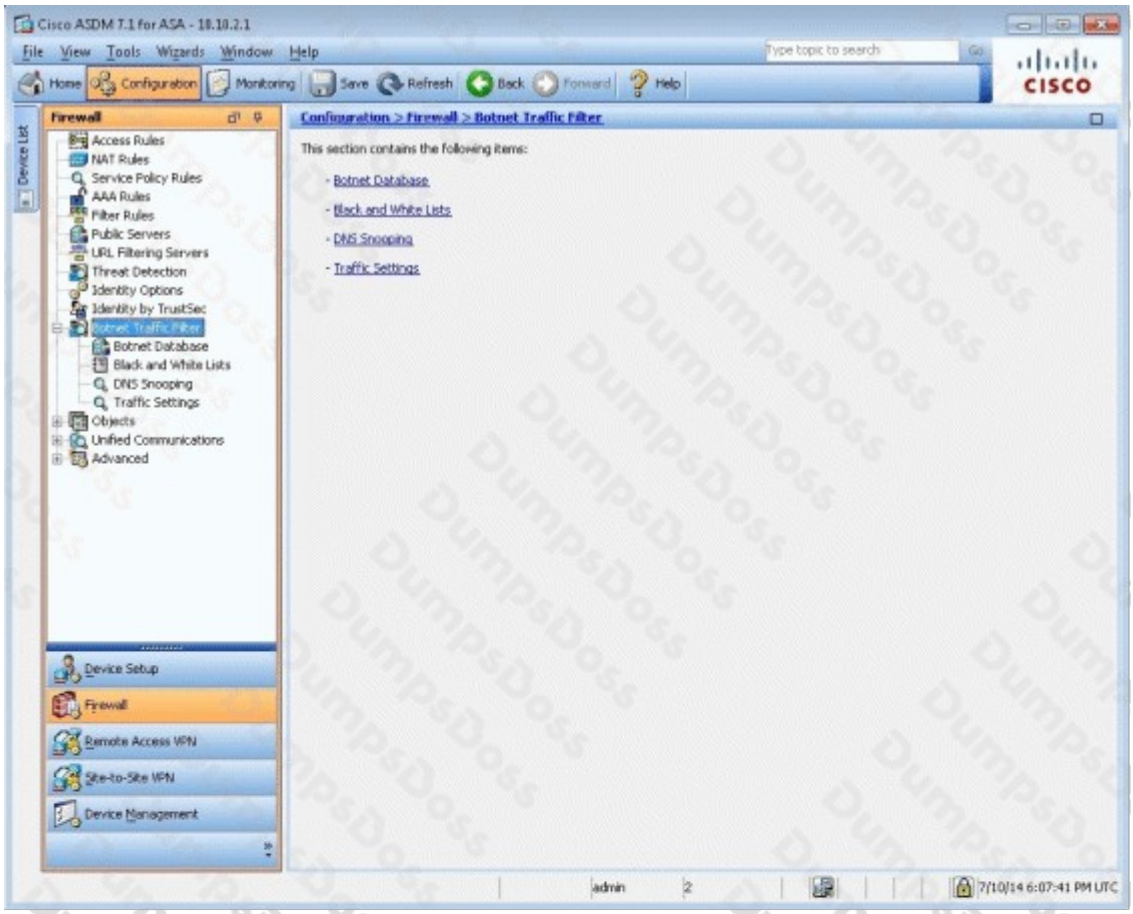

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Logging
Real-Time Log Viewer
Log Buffer
Monitoring > Logging > Real-Time Log Viewer
Real-Time Log Viewer
Click the View button below to start displaying syslog messages in real time. Select the desired logging level to see messages at that severity or higher.
Logging Level:
Debugging
Buffer Limit:
1000
View...
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Data Refreshed Successfully.
student
15

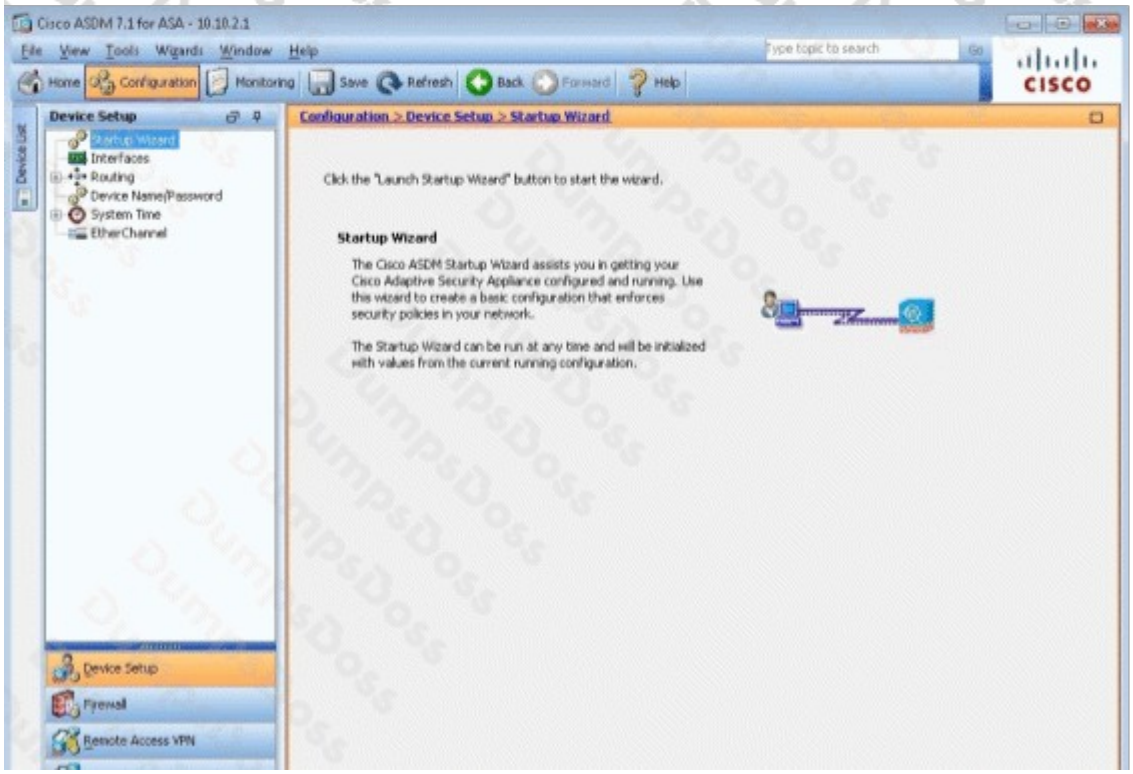

Real-Time Log Viewer - 10.10.2.1
File Tools Window Help
Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help
Filter By: Filter Build Filter Show All Find:
Severity Date Time Syslog SourceIP SourcePort DestinationIP Destination Description
6 Nov 3 2015 15:44:18 302017 208.90.57.75 443 10.10.1.50 62270 Teardown TCP conenction 81
6 Nov 3 2015 15:44:18 302017 10.10.2.40 0 10.10.1.1 0 Teardown TCP conenction for
6 Nov 3 2015 15:44:18 302017 10.10.2.40 0 10.10.1.1 0 Built inbound ICMP connectio
6 Nov 3 2015 15:44:18 302017 10.10.9.50 62270 208.90.57.75 443 Built outbound TCP connectio
6 Nov 3 2015 15:44:18 302017 10.10.9.50 62270 208.90.57.75 443 Built outbound TCP connectio
6 Nov 3 2015 15:44:18 302017 10.10.9.50 62270 208.90.57.75 443 Built outbound TCP connectio
6 Nov 3 2015 15:44:18 302017 23.72.38.160 80 172.16.1.55 12730 Teardown TCP conenction 81
6 Nov 3 2015 15:44:18 302017 172.16.1.55 12730 23.72.38.160 80 Built outbound TCP connectio
6 Nov 3 2015 15:44:18 302017 10.10.2.40 0 10.10.1.1 0 Teardown ICMP connection fo
6 Nov 3 2015 15:44:18 302017 172.16.1.55 12730 23.72.38.160 80 Built outbound TCP connectio
6 Nov 3 2015 15:44:18 302017 10.10.2.40 0 10.10.1.1 0 Teardown ICMP connection fo
6 Nov 3 2015 15:44:18 302017 209.165.200.233 53 10.10.3.20 65394 Teardown UDP connection 81
Syslog Details
Severity: 4 (Warnings) Date: May 15 2014 Source IP: 10.10.9.17 Source Port: 1057
Syslog ID: 338006 Time: 21:49:30 Destination IP: 41.109.132.70 Destination Port: 80
Description: Dynamic Filter dropped blacklisted TCP traffic from inside:10.10.9.17/1057 (192.0.2.178/1057) to outside:41.109.132.70/80 (41.109.132.70/80), destination 41.109.132.70 resolved from dynamic list: bot-sparta.no-ip.org, threat-level: very-high,
Explanation Recommended Action Details
Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging
Scenario TOPOLOGY


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
NAC Session Summary
Protocol Statistics
VLAN Mapping Sessions
Clientless SSL VPN
VPN Connection Graphs
IPsec Tunnels
Sessions
WSA Sessions
Monitoring > VPN > VPN Statistics > Sessions
Type Active Cumulative Peak Concurrent Inactive
Clientless VPN 0 8 2
Browser 0 8 2
Site-to-Site VPN 1 2 1
IKEv1 IPsec 1 2 1
Filter By: IPsec Site-to-Site -- All Sessions -- Filter
ConnectionProfileIPAddress ProtocolEncryption LoginTimeDuration BytesTxBytesRx
Details
Logout
Ping
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.
Logout By: -- All Sessions -- Logout Sessions
Refresh
Interfaces
VPN
Botnet Traffic Filter
IPS
Routing
Properties
Logging

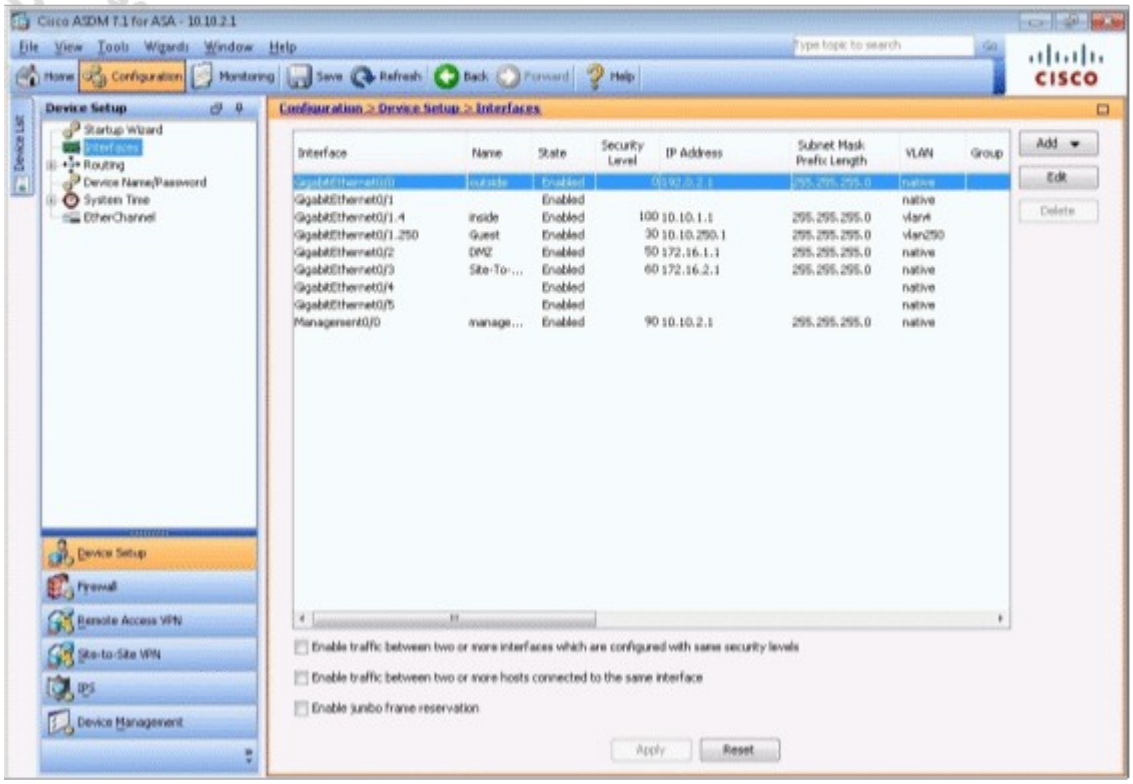

Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Properties
AAA Servers
Device Access
AAA Local Locked Out Us
Authenticated Users
ASDM/HTTPS/Telnet/SSH
Monitoring > Properties > AAA Servers
AAA Servers
Each row represents one AAA Server. Select a server in the table to see the full statistics in the box below.

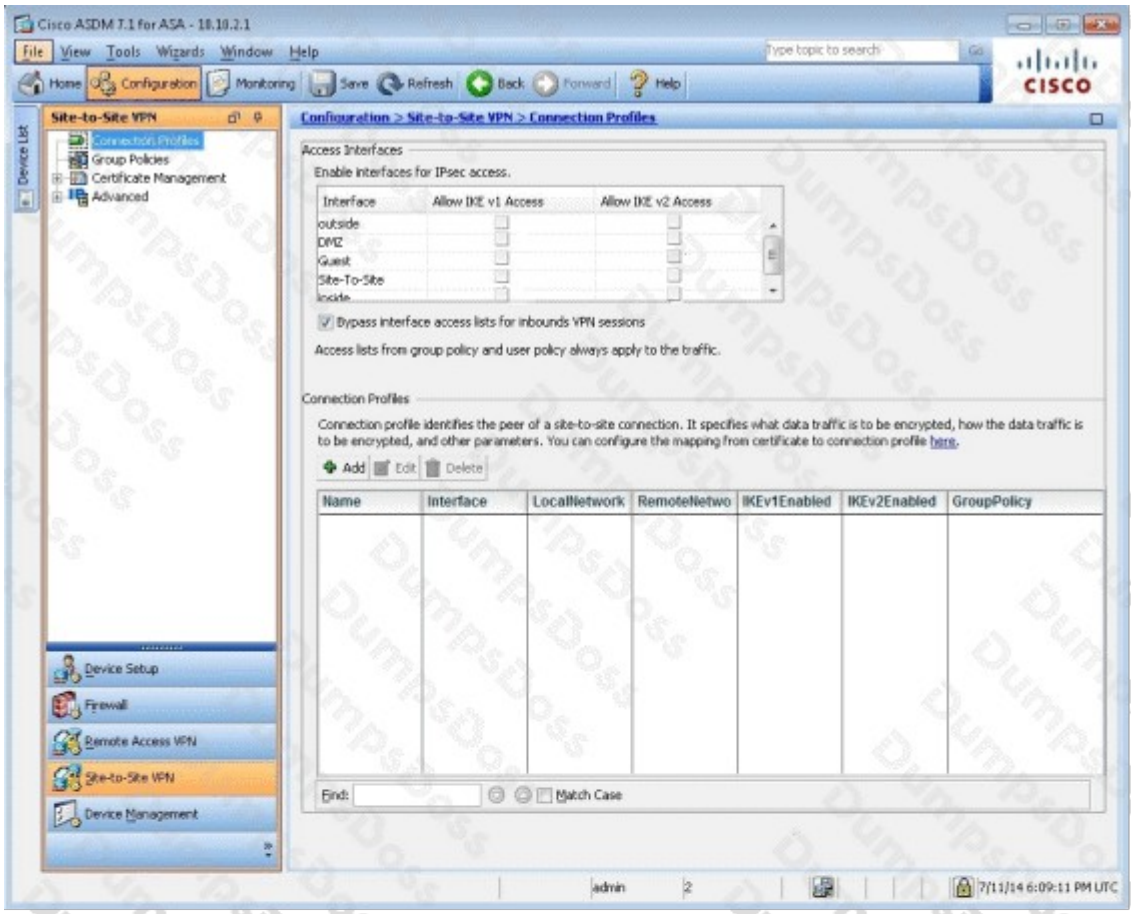

Properties
AAA Servers
Device Access
AAA Local Locked Out Us
Authenticated Users
ASDM/HTTPS/Telnet/SSH
Connection Graphs
Perfmon
Xlates
CRL
DNS Cache
Failover
Status
Graphs
Identity
AD Agent
Groups
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Monitoring > Properties > AAA Servers
AAA Servers
Each row represents one AAA Server. Select a server in the table to see the full statistics in the box below.
Server Group
Protocol
IP Address
Status
LOCAL
Local database
None
Active
Server port: None
Number of pending requests 0
Average round trip time 0ms
Number of authentication requests 1
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1
Number of rejects 0
Number of challenges 0
Clear Server Statistics
Update Server Status...
Refresh
Last Updated: 6/27/14 1:07:54 PM
Data Refreshed
Data Refreshed Successfully.
student
15
6/27/14 8:07:31 PM UTC

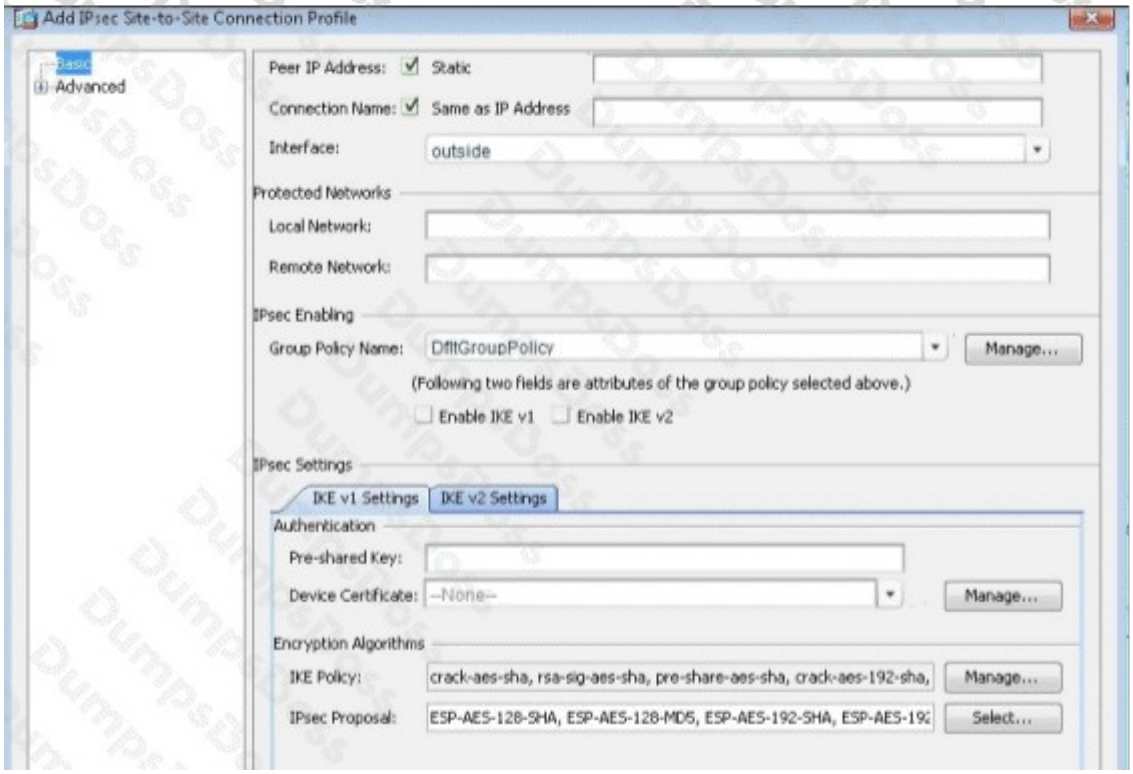

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Unified Communications
Advanced
Configuration > Firewall > Botnet Traffic Filter
This section contains the following items:
- Botnet Database
- Black and White Lists
- DNS Snooping
- Traffic Settings
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
admin
2
7/10/14 6:07:41 PM UTC


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interfaces
Routing
Device Name/Password
System Time
EtherChannel
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" button to start the wizard.
Startup Wizard
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.
Device Setup
Firewall
Remote Access VPN

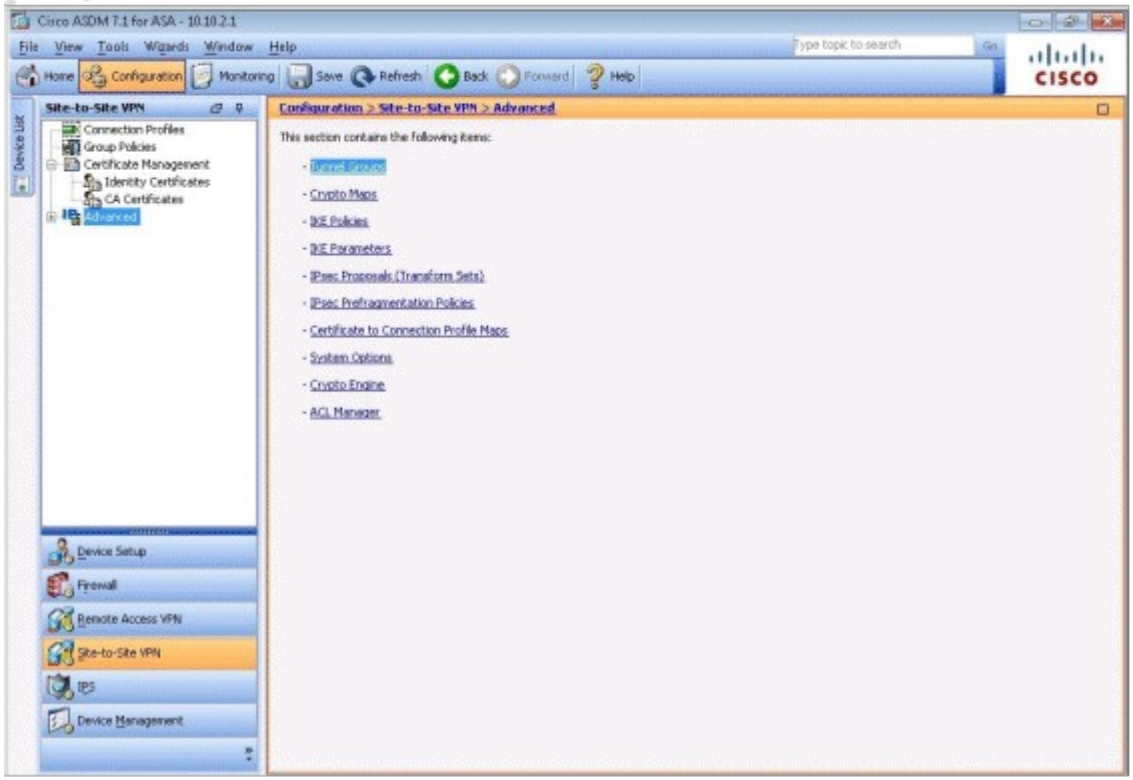

Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Launch Startup Wizard
admin
2
7/10/14 6:03:51 PM UTC

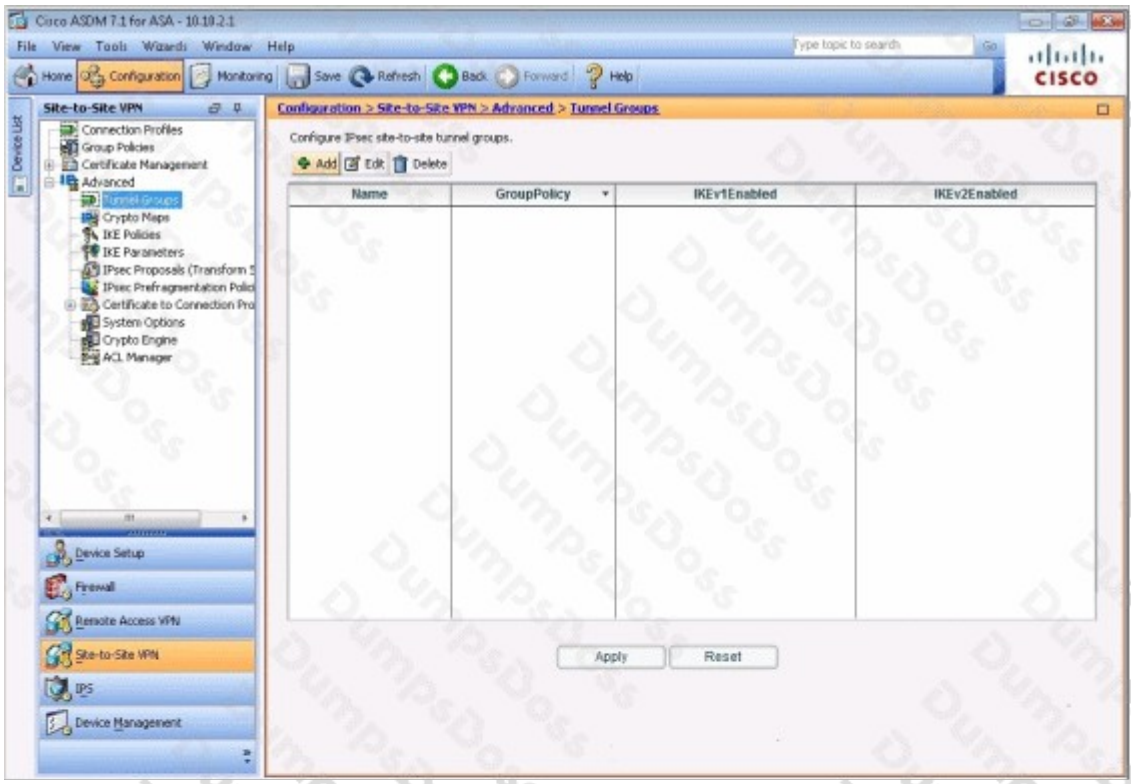

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interfaces
Routing
Device Name/Password
System Time
EtherChannel
Configuration > Device Setup > Interfaces
Interface Name State Security Level IP Address Subnet Mask Prefix Length VLAN Group
GigabitEthernet0/0 outside Enabled 0 10.10.2.1 255.255.255.0 native
GigabitEthernet0/1 Enabled native
GigabitEthernet0/1.4 inside Enabled 100 10.10.1.1 255.255.255.0 vlan4
GigabitEthernet0/1.250 Guest Enabled 30 10.10.250.1 255.255.255.0 vlan250
GigabitEthernet0/2 DMZ Enabled 50 172.16.1.1 255.255.255.0 native
GigabitEthernet0/3 Site-To-... Enabled 60 172.16.2.1 255.255.255.0 native
GigabitEthernet0/4 Enabled native
GigabitEthernet0/5 Enabled native
Management0/0 manage... Enabled 90 10.10.2.1 255.255.255.0 native
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management

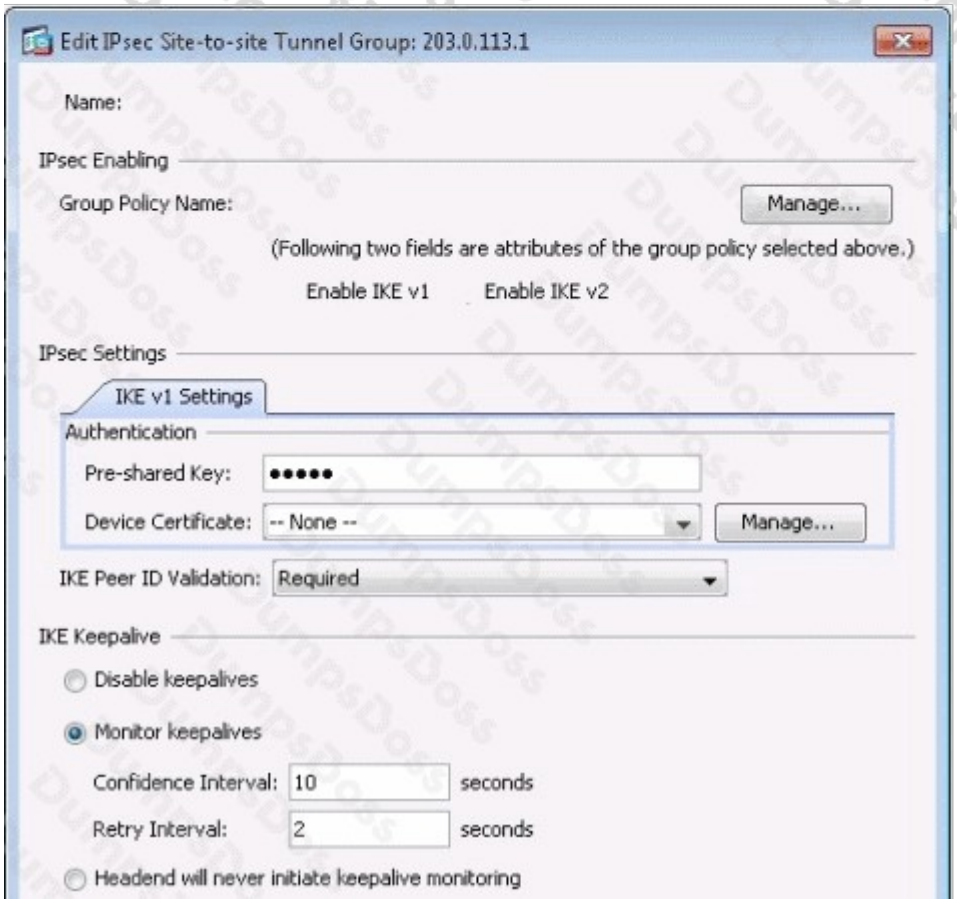

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Configuration > Site-to-Site VPN > Connection Profiles
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow IKE v1 Access
Allow IKE v2 Access
outside
DMZ
Guest
Site-To-Site
Bypass interface access lists for inbounds VPN sessions
Access lists from group policy and user policy always apply to the traffic.
Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile here.
Add
Edit
Delete
Name
Interface
LocalNetwork
RemoteNetwo
IKEv1Enabled
IKEv2Enabled
GroupPolicy
Find:
Match Case
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
admin
2
7/11/14 6:09:11 PM UTC


Add IPsec Site-to-Site Connection Profile
Basic
Advanced
Peer IP Address:
Static
Connection Name:
Same as IP Address
Interface:
outside
Protected Networks
Local Network:
Remote Network:
IPsec Enabling
Group Policy Name:
DfltGrpPolicy
Manage...
(Following two fields are attributes of the group policy selected above.)
Enable IKE v1
Enable IKE v2
IPsec Settings
IKE v1 Settings
IKE v2 Settings
Authentication
Pre-shared Key:
Device Certificate:
--None--
Manage...
Encryption Algorithms
IKE Policy:
crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha,
Manage...
IPsec Proposal:
ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192
Select...

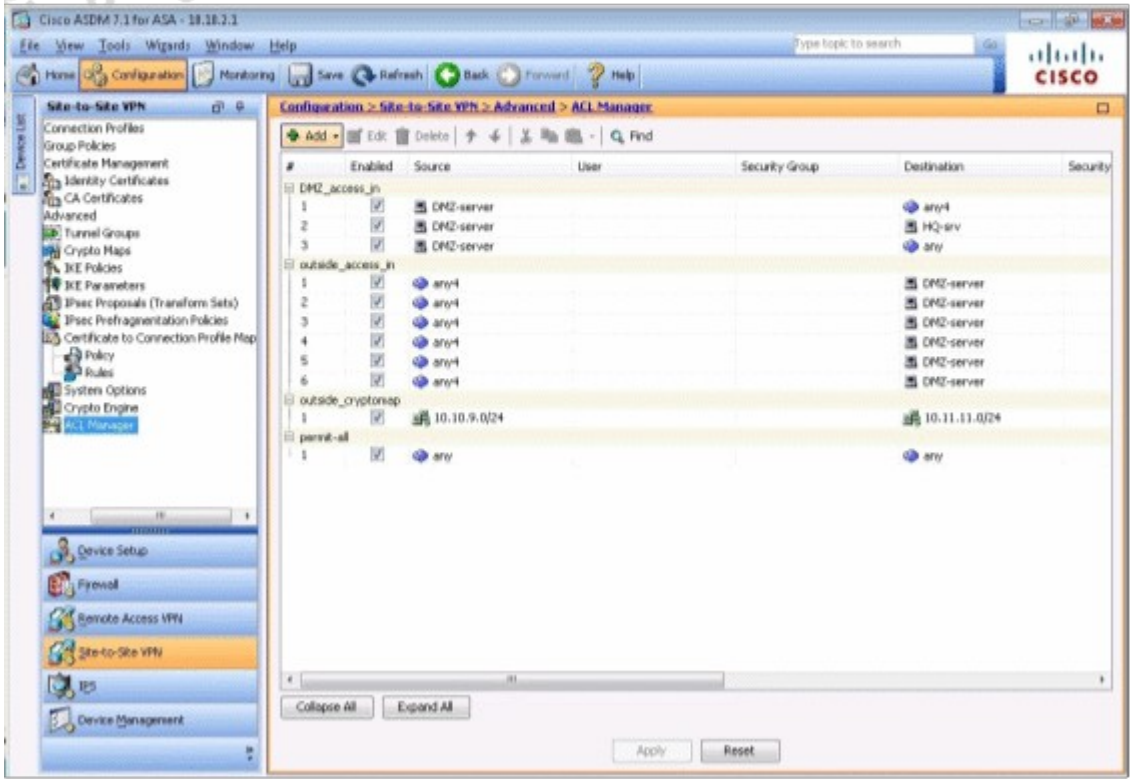

IKE Policy:
crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha,
Manage...
IPsec Proposal:
ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192
Select...
OK
Cancel
Help
Find:
Next
Previous

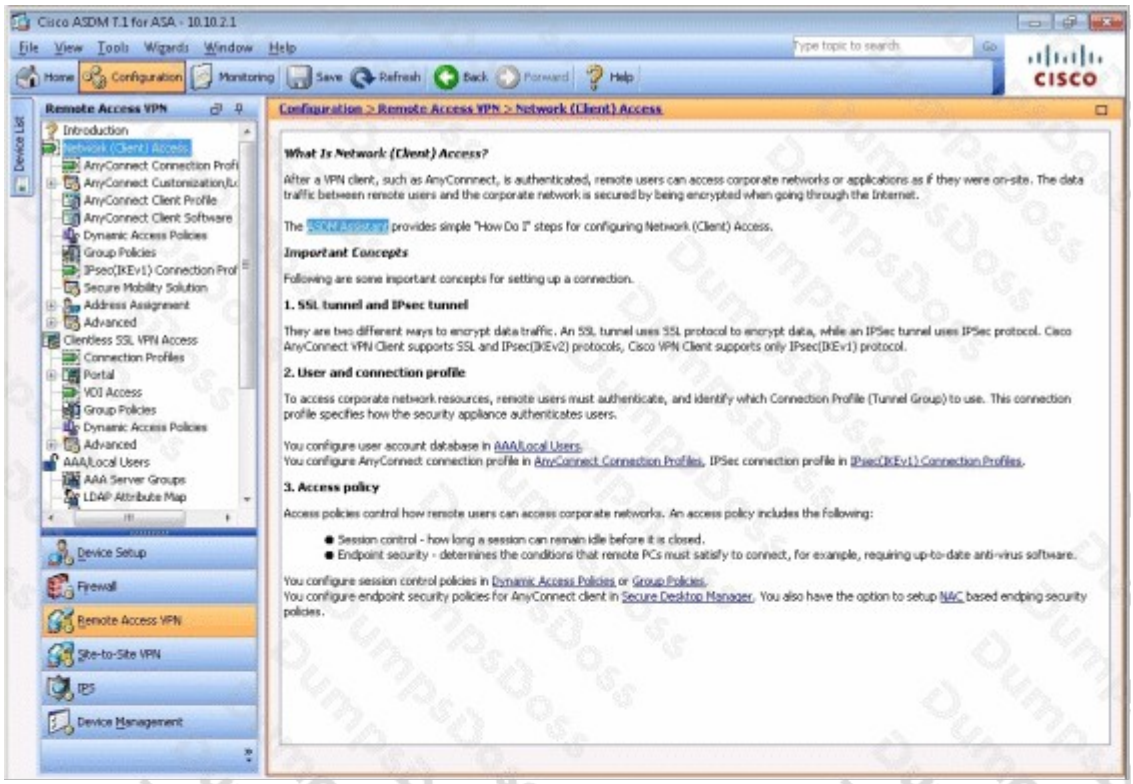

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Identity Certificates
CA Certificates
Advanced
Configuration > Site-to-Site VPN > Advanced
This section contains the following items:
- Crypto Maps
- IKE Policies
- IKE Parameters
- IPsec Proposals (Transform Sets)
- IPsec Prefragmentation Policies
- Certificate to Connection Profile Maps
- System Options
- Crypto Engine
- ACL Manager
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management

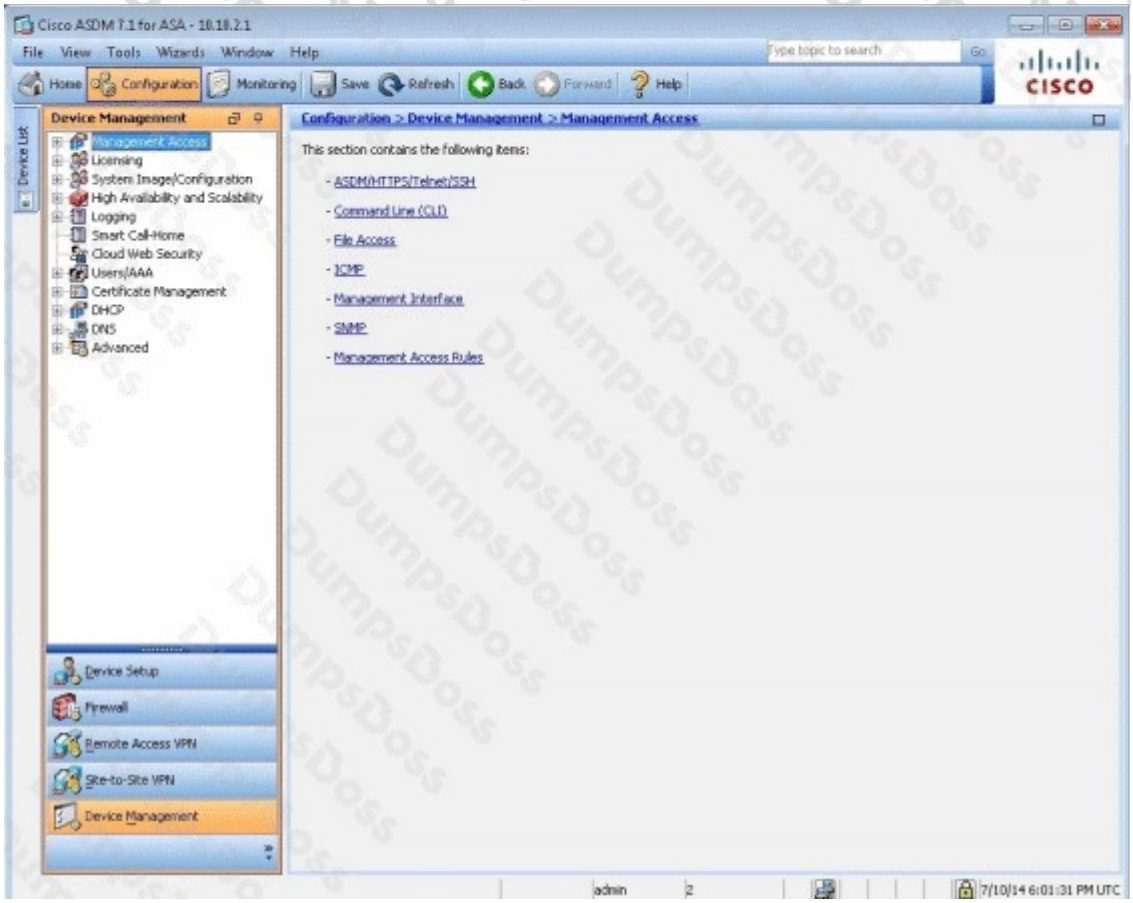

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Prefragmentation Policies
Certificate to Connection Profile Maps
System Options
Crypto Engine
ACL Manager
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Site-to-Site VPN > Advanced > Tunnel Groups
Configure IPsec site-to-site tunnel groups.
Add Edit Delete
Name
GroupPolicy
IKEv1Enabled
IKEv2Enabled
Apply
Reset

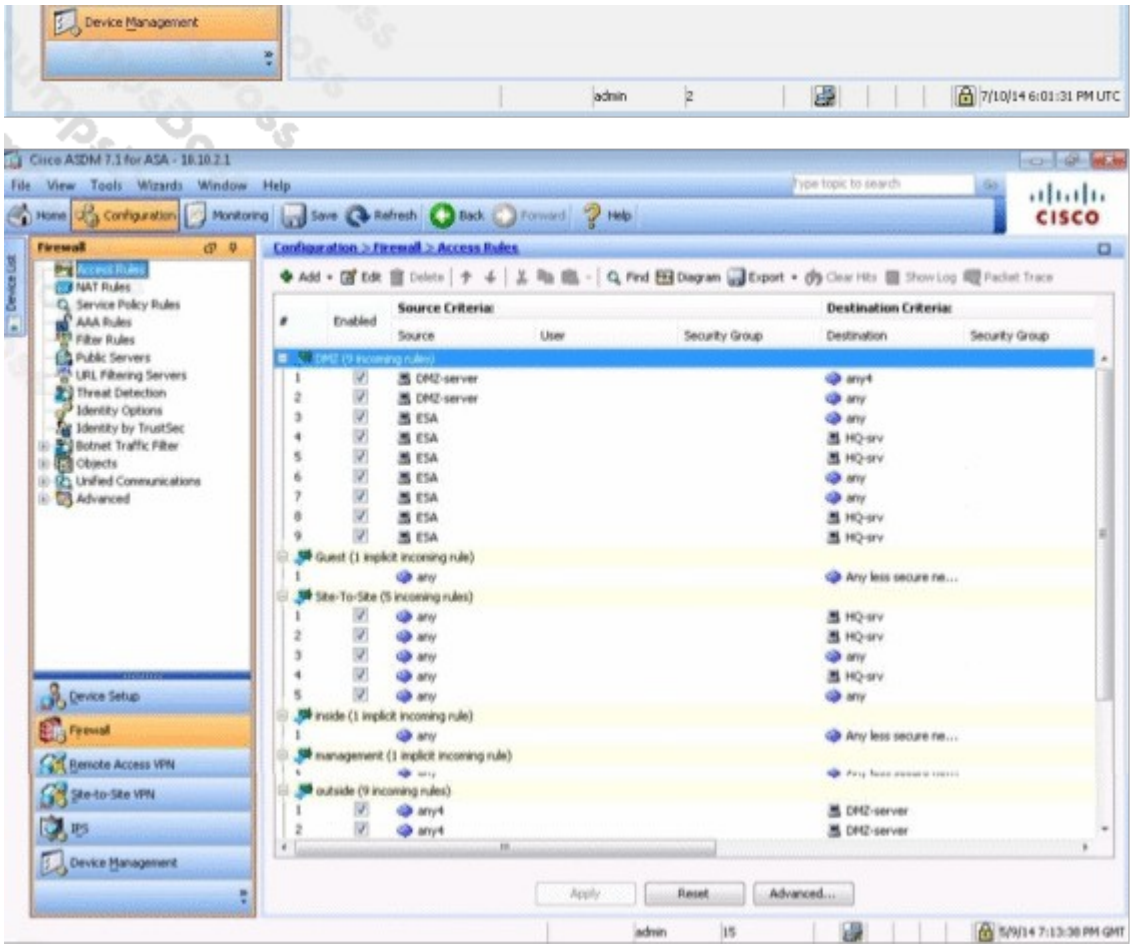

Edit IPsec Site-to-site Tunnel Group: 203.0.113.1
Name:
IPsec Enabling
Group Policy Name:
Manage...
(Following two fields are attributes of the group policy selected above.)
Enable IKE v1
Enable IKE v2
IPsec Settings
IKE v1 Settings
Authentication
Pre-shared Key:
Device Certificate:
-- None --
Manage...
IKE Peer ID Validation:
Required
IKE Keepalive
Disable keepalives
Monitor keepalives
Confidence Interval:
10
seconds
Retry Interval:
2
seconds
Headend will never initiate keepalive monitoring

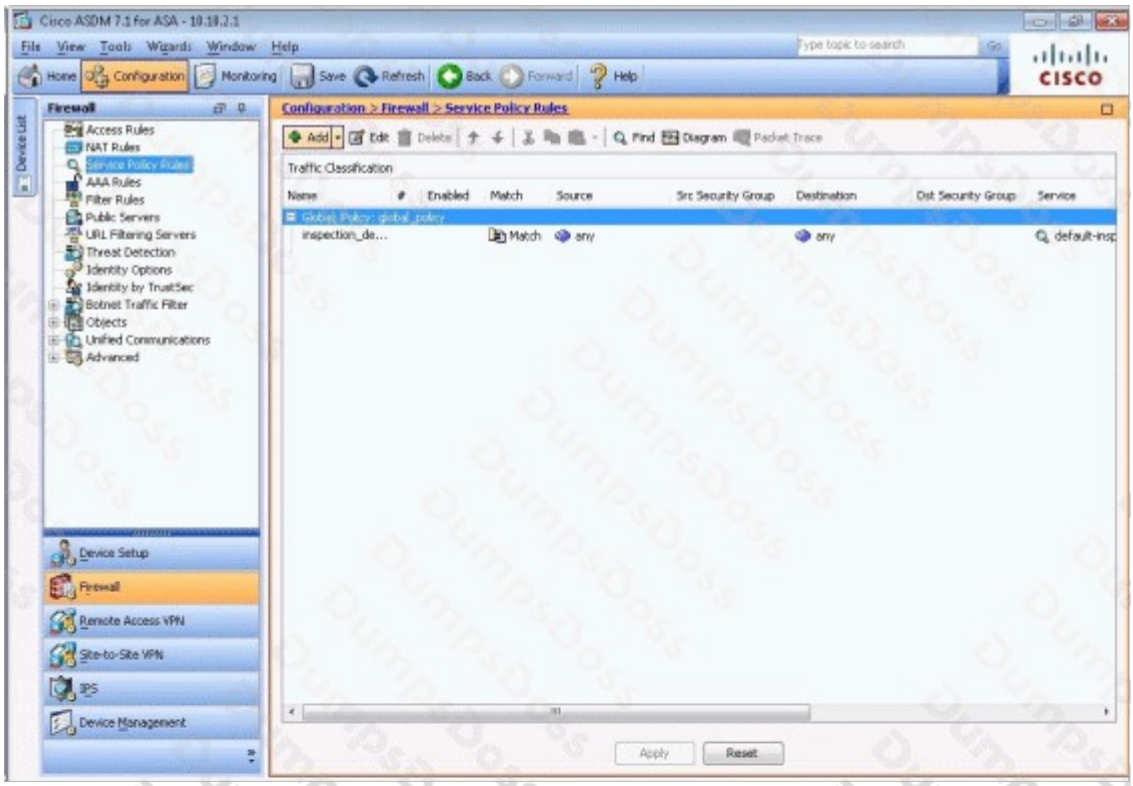

Retry Interval:
2
seconds
Headend will never initiate keepalive monitoring

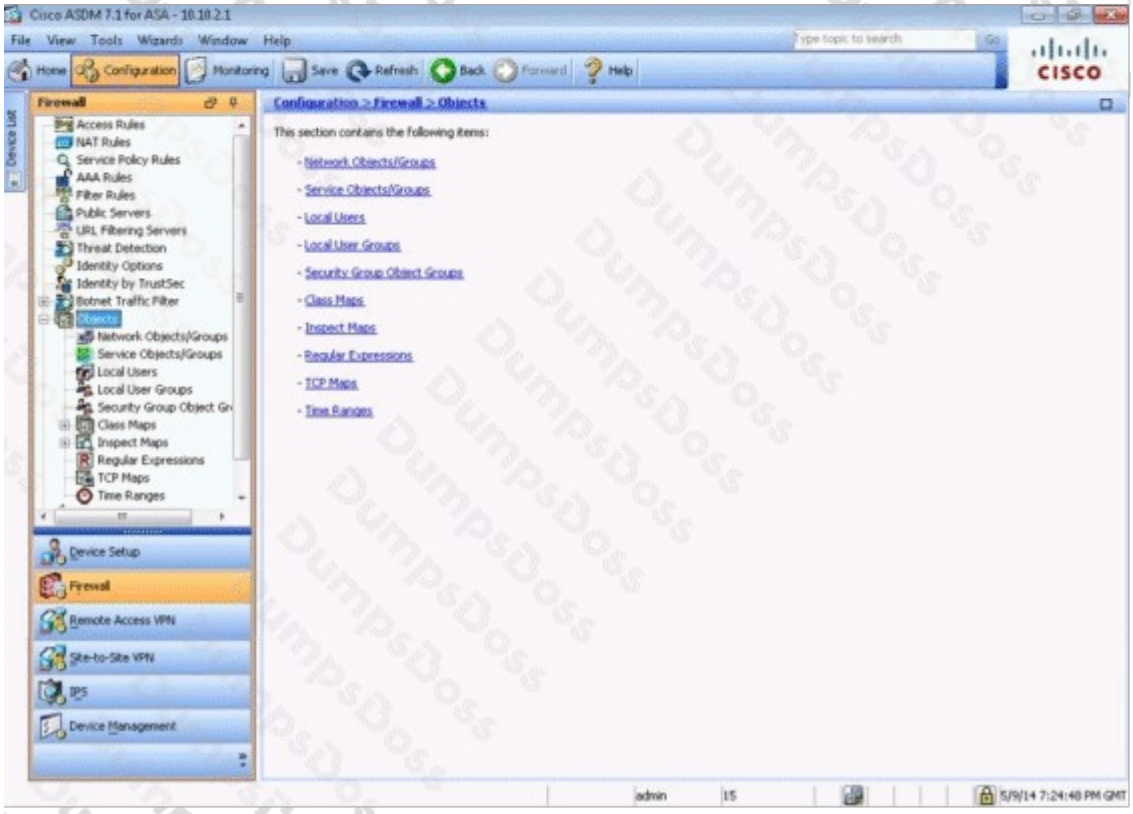

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Identity Certificates
CA Certificates
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile Map
Policy
Rules
System Options
Crypto Engine
ACL Manager
Configuration > Site-to-Site VPN > Advanced > ACL Manager
Add Edit Delete Find
Enabled Source User Security Group Destination Security
DMZ_access_in
1 DMZ-server any4
2 DMZ-server HQ-srv
3 DMZ-server any
outside_access_in
1 any4 DMZ-server
2 any4 DMZ-server
3 any4 DMZ-server
4 any4 DMZ-server
5 any4 DMZ-server
6 any4 DMZ-server
outside_cryptomap
1 10.10.9.0/24 10.11.11.0/24
permit-all
1 any any
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Collapse All
Expand All
Apply
Reset

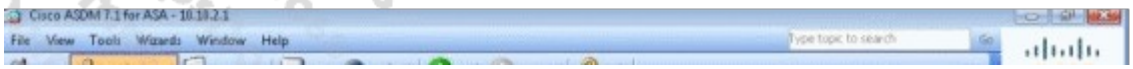

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profi
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Prof
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
VDI Access
Group Policies
Dynamic Access Policies
Advanced
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
The VPN Assistant provides simple "How Do I" steps for configuring Network (Client) Access.
Important Concepts
Following are some important concepts for setting up a connection.
1. SSL tunnel and IPsec tunnel
There are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPSec tunnel uses IPSec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(IKEv2) protocols, Cisco VPN Client supports only IPsec(IKEv1) protocol.
2. User and connection profile
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in AAA/Local Users.
You configure AnyConnect connection profile in AnyConnect Connection Profiles, IPSec connection profile in IPsec(IKEv1) Connection Profiles.
3. Access policy
Access policies control how remote users can access corporate networks. An access policy includes the following:
Session control - how long a session can remain idle before it is closed.
Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
You configure session control policies in Dynamic Access Policies or Group Policies.
You configure endpoint security policies for AnyConnect client in Secure Desktop Manager. You also have the option to setup NAC based endpoint security policies.

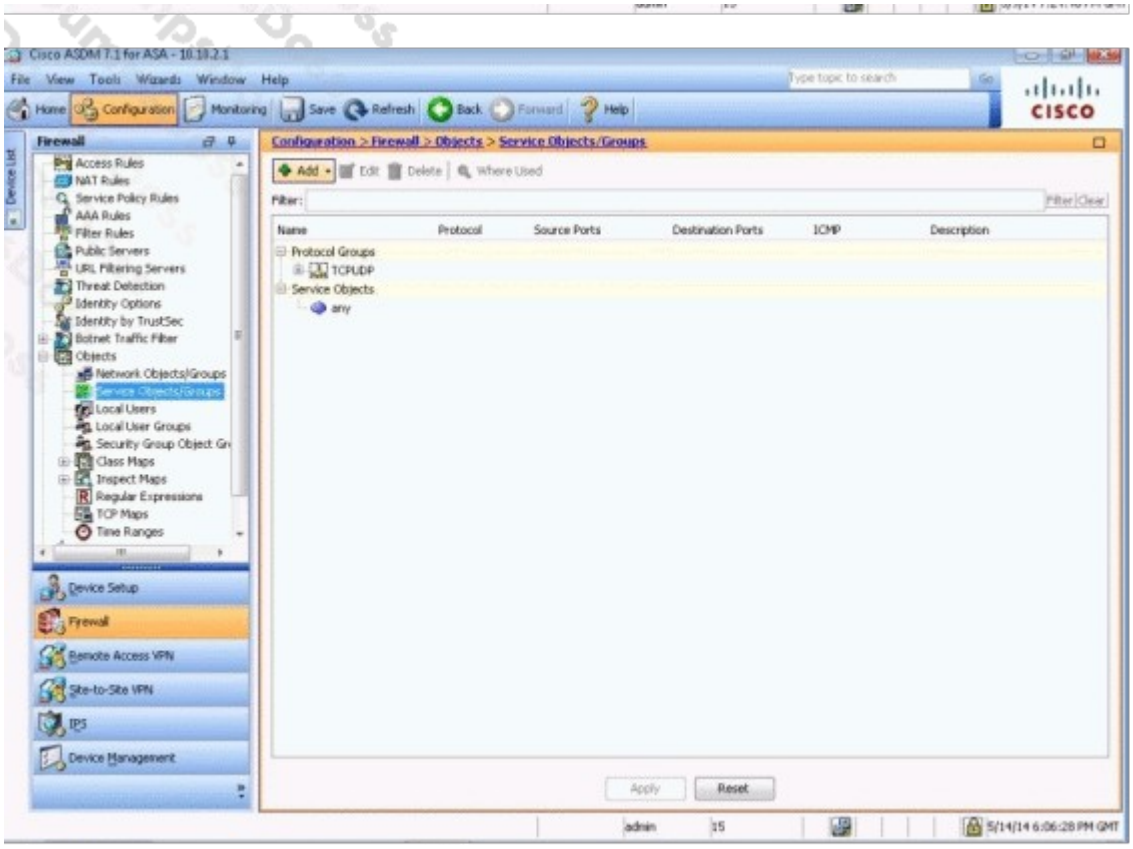

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
DHCP
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Management Access
This section contains the following items:
- ASDM/HTTPS/Telnet/SSH
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- SNMP
- Management Access Rules
admin
7/10/14 6:01:31 PM UTC

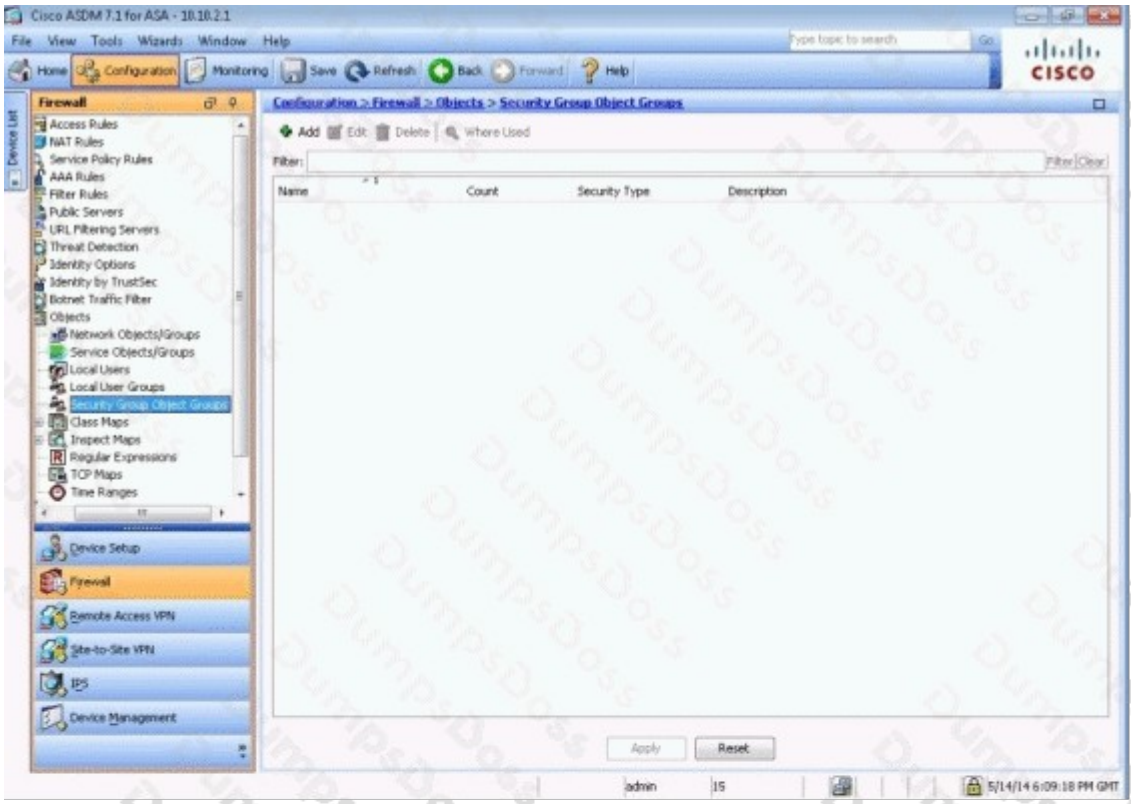

Device Management
admin
2
7/10/14 6:01:31 PM UTC
Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
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
DMZ (9 incoming rules)
1 DMZ-server any4
2 DMZ-server any
3 ESA any
4 ESA HQ-srv
5 ESA HQ-srv
6 ESA any
7 ESA any
8 ESA HQ-srv
9 ESA HQ-srv
Guest (1 implicit incoming rule)
1 any Any less secure ne...
Site-To-Site (5 incoming rules)
1 any HQ-srv
2 any HQ-srv
3 any any
4 any HQ-srv
5 any any
inside (1 implicit incoming rule)
1 any Any less secure ne...
management (1 implicit incoming rule)
outside (9 incoming rules)
1 any4 DMZ-server
2 any4 DMZ-server
Apply Reset Advanced...
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
admin 15
5/9/14 7:13:38 PM GMT

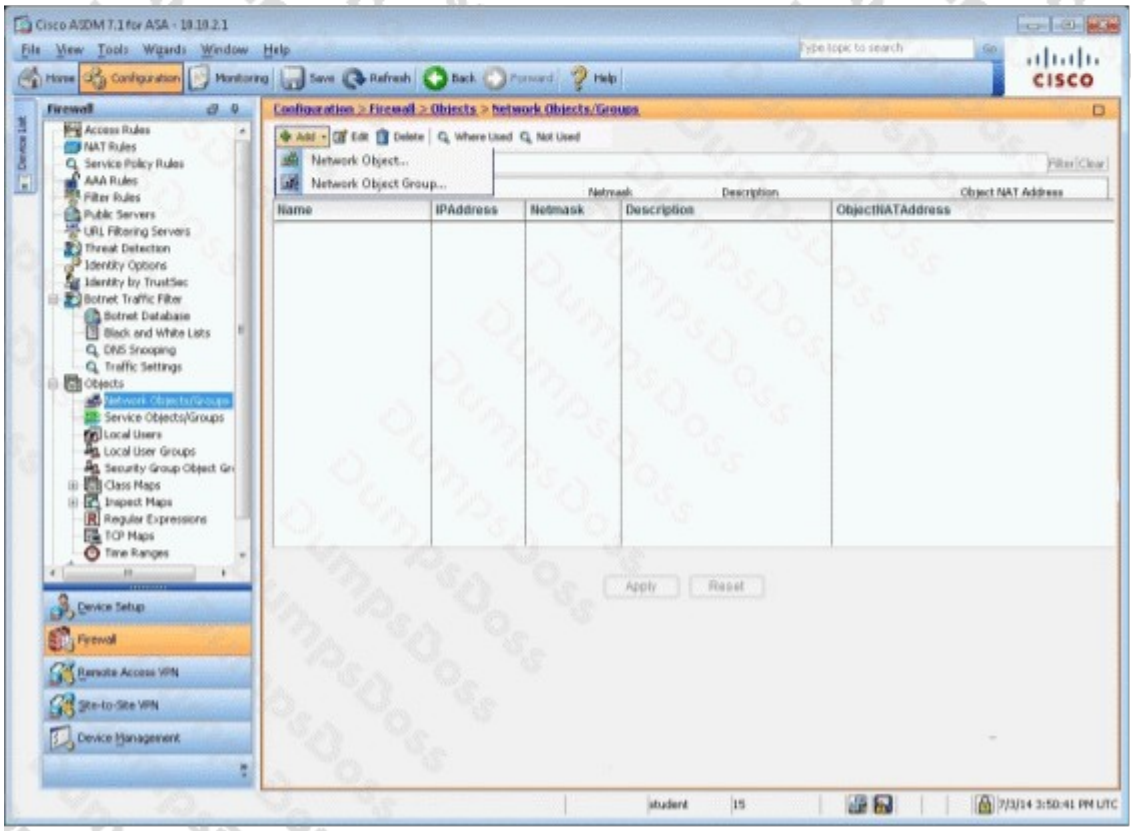

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security Group Destination Dst Security Group Service
Global Policy: global_policy
inspection_de... Match any any default-insp
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Apply Reset

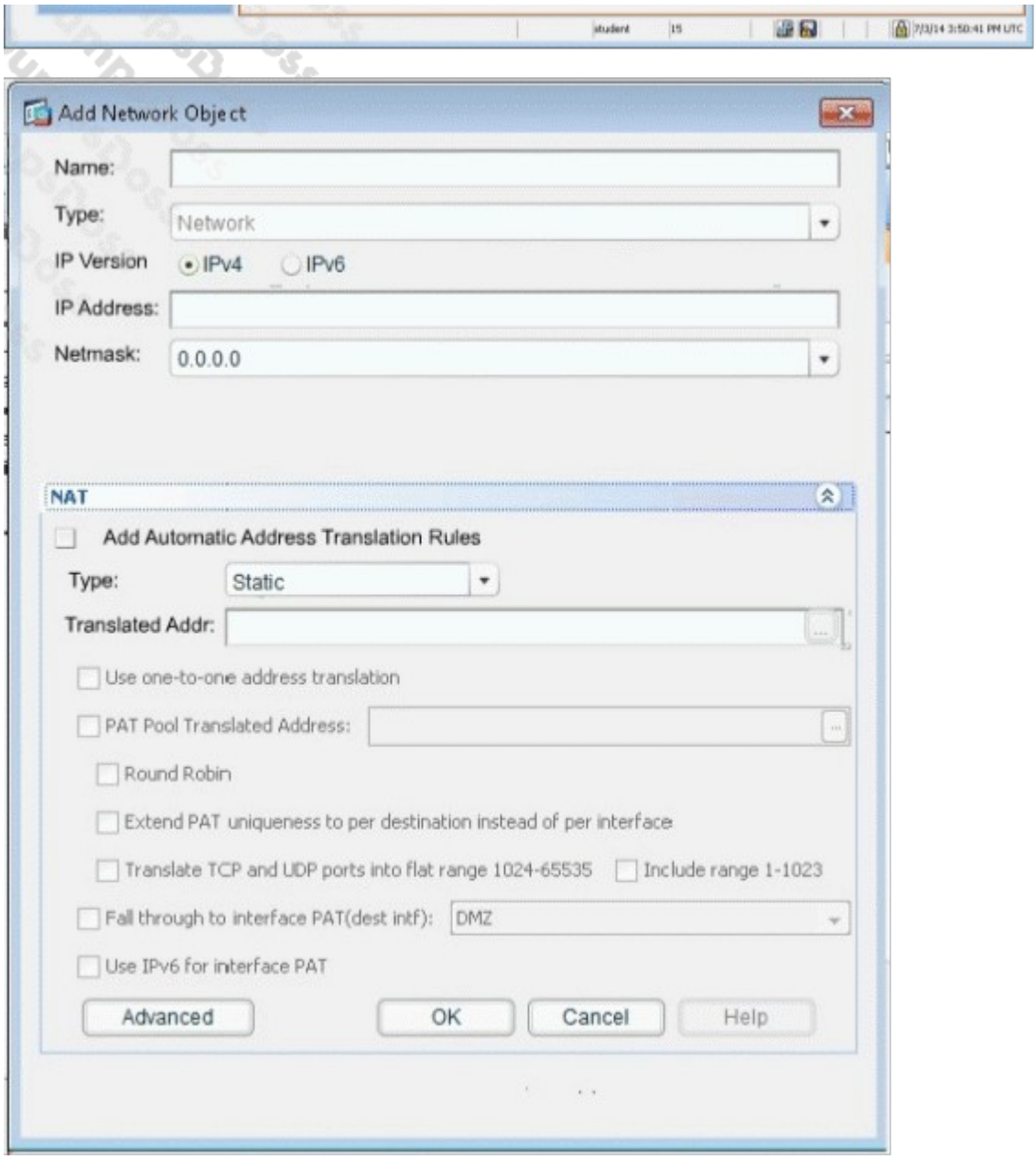

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Configuration > Firewall > Objects
This section contains the following items:
- Network Objects/Groups
- Service Objects/Groups
- Local Users
- Local User Groups
- Security Group Object Groups
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
admin 15 5/9/14 7:24:40 PM GMT

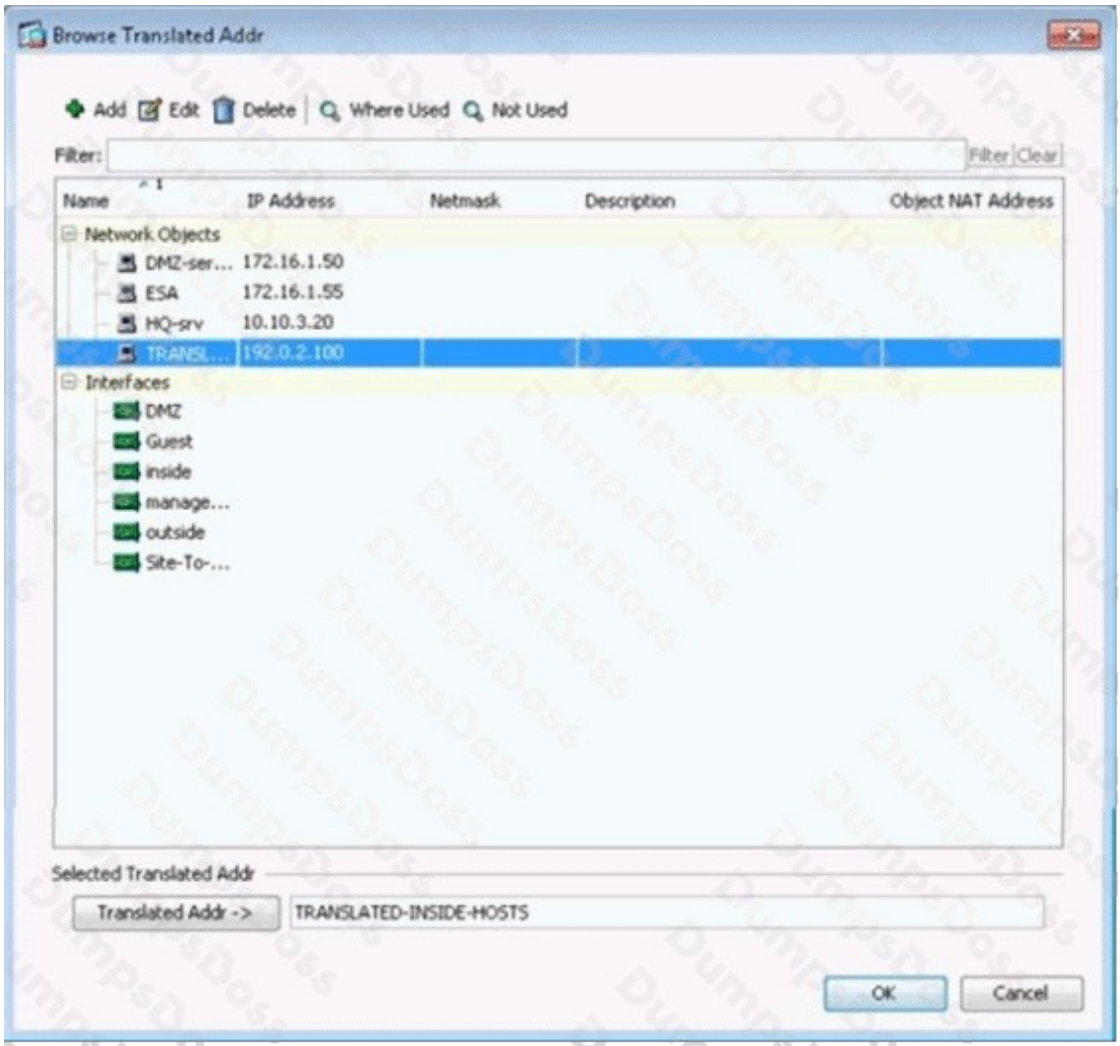

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help

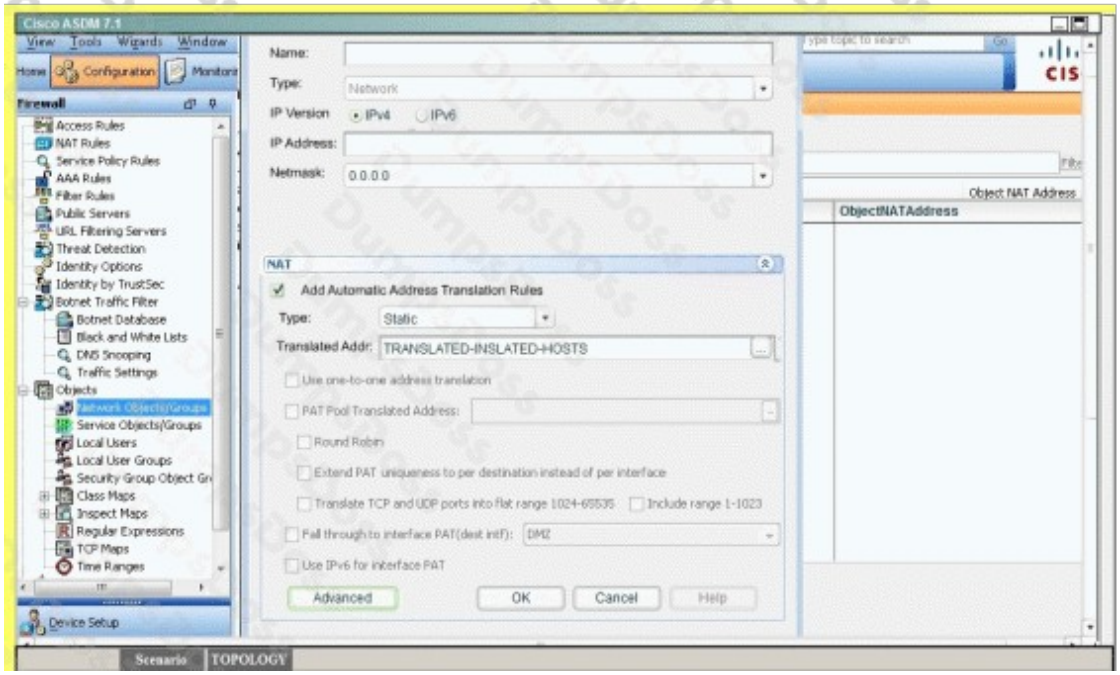

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Objects > Service Objects/Groups
Add Edit Delete Where Used
Filter:
Filter Clear
Name
Protocol
Source Ports
Destination Ports
ICMP
Description
Protocol Groups
TCPUDP
Service Objects
any
Apply
Reset
admin
15
5/14/14 6:06:28 PM GMT


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
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
Security Group Object Groups
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 > Security Group Object Groups
Add Edit Delete Where Used
Filter:
Filter Clear
Name
Count
Security Type
Description
Apply
Reset
admin
15
5/14/14 6:09:18 PM GMT

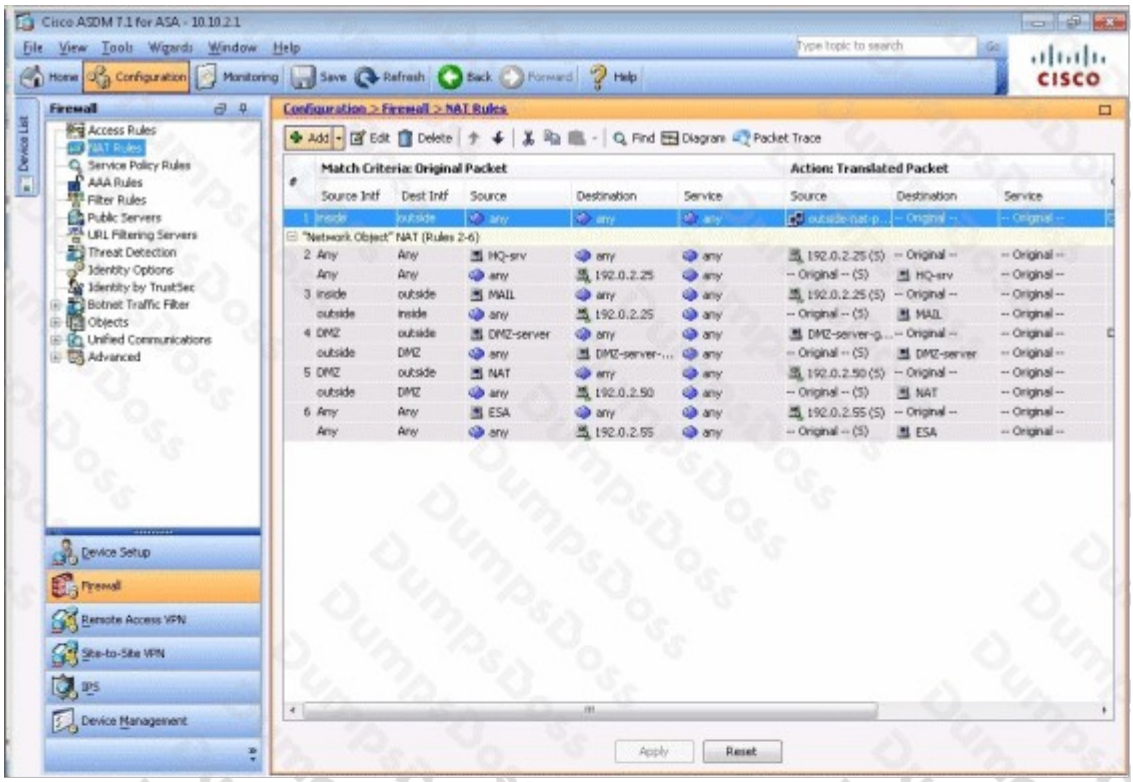

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Firewall > Objects > Network Objects/Groups
Add Edit Delete Where Used Not Used
Network Object...
Network Object Group...
Filter Clear
Name
IPAddress
Netmask
Description
ObjectNATAddress
Apply
Reset
student
15
7/3/14 3:50:41 PM UTC

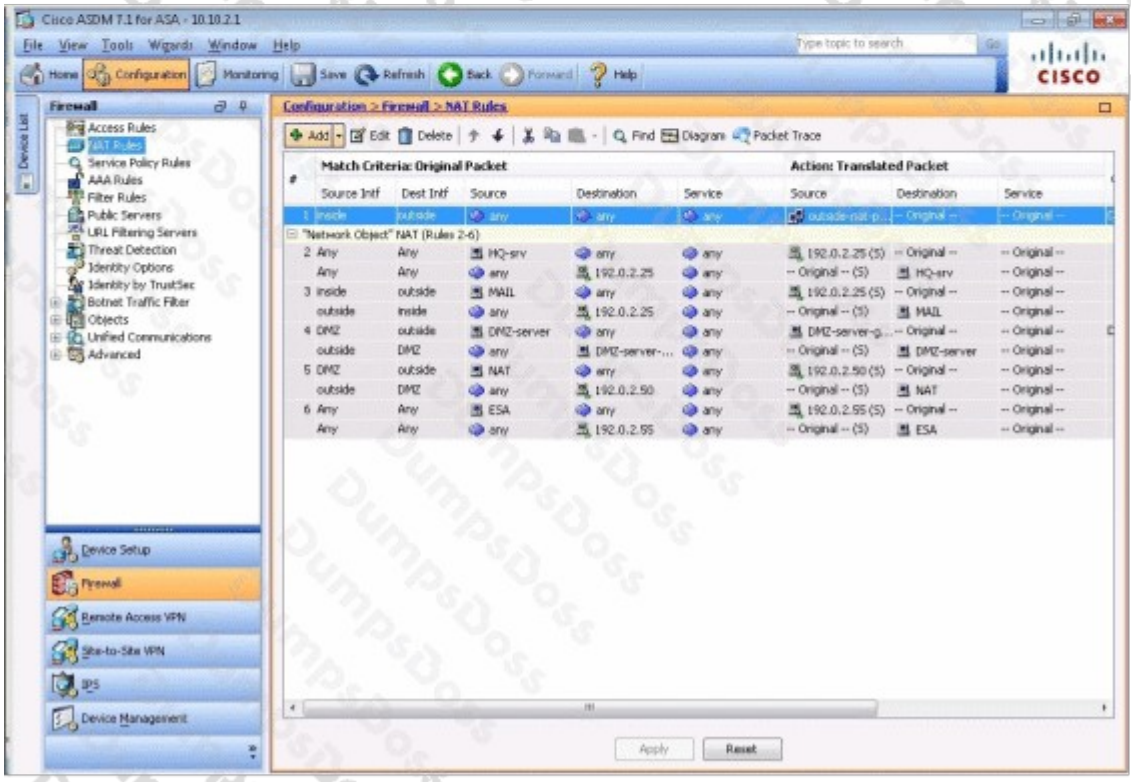

Add Network Object
Name:
Type:
Network
IP Version
IPv4
IPv6
IP Address:
Netmask:
0.0.0.0
NAT
Add Automatic Address Translation Rules
Type:
Static
Translated Addr:
Use one-to-one address translation
PAT Pool Translated Address:
Round Robin
Extend PAT uniqueness to per destination instead of per interface
Translate TCP and UDP ports into flat range 1024-65535
Include range 1-1023
Fall through to interface PAT(dest intf):
DMZ
Use IPv6 for interface PAT
Advanced
OK
Cancel
Help


Browse Translated Addr
Add
Edit
Delete
Where Used
Not Used
Filter:
Filter
Clear
Name
IP Address
Netmask
Description
Object NAT Address
Network Objects
DMZ-ser...
172.16.1.50
ESA
172.16.1.55
HQ-srv
10.10.3.20
TRANSL...
192.0.2.100
Interfaces
DMZ
Guest
inside
manage...
outside
Site-To-...
Selected Translated Addr
Translated Addr ->
TRANSLATED-INSIDE-HOSTS
OK
Cancel

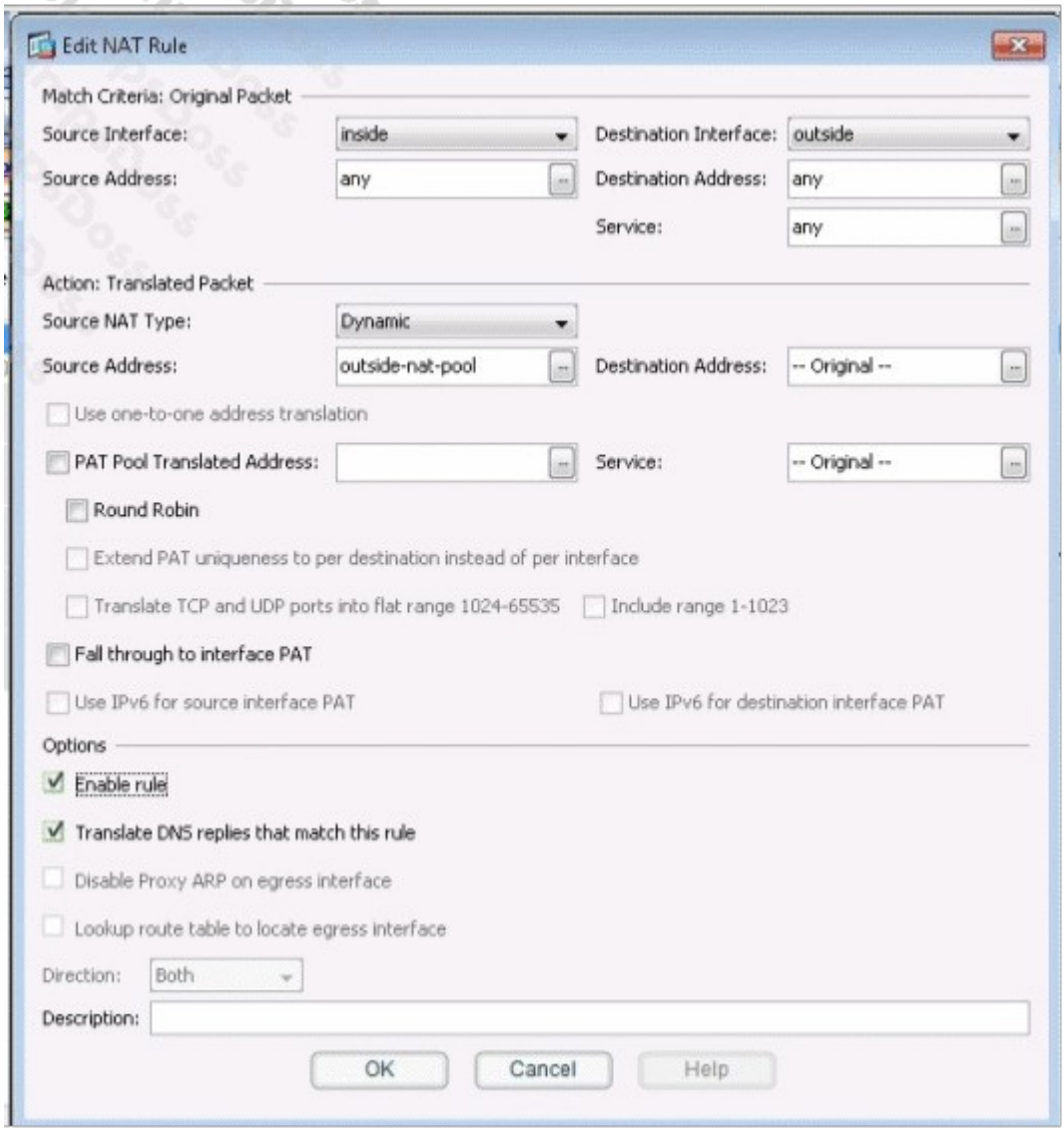

Cisco ASDM 7.1
View
Tools
Wizards
Window
Configuration
Monitoring
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Device Setup
Name:
Type:
Network
IP Version
IPv4
IPv6
IP Address:
Netmask:
0.0.0.0
NAT
Add Automatic Address Translation Rules
Type:
Static
Translated Addr:
TRANSLATED-INSLATED-HOSTS
Use one-to-one address translation
PAT Pool Translated Address:
Round Robin
Extend PAT uniqueness to per destination instead of per interface
Translate TCP and UDP ports into flat range 1024-65535
Include range 1-1023
Fall through to interface PAT(dest intf):
DMZ
Use IPv6 for interface PAT
Advanced
OK
Cancel
Help
Object NAT Address
ObjectNATAddress
Scenario
TOPOLOGY

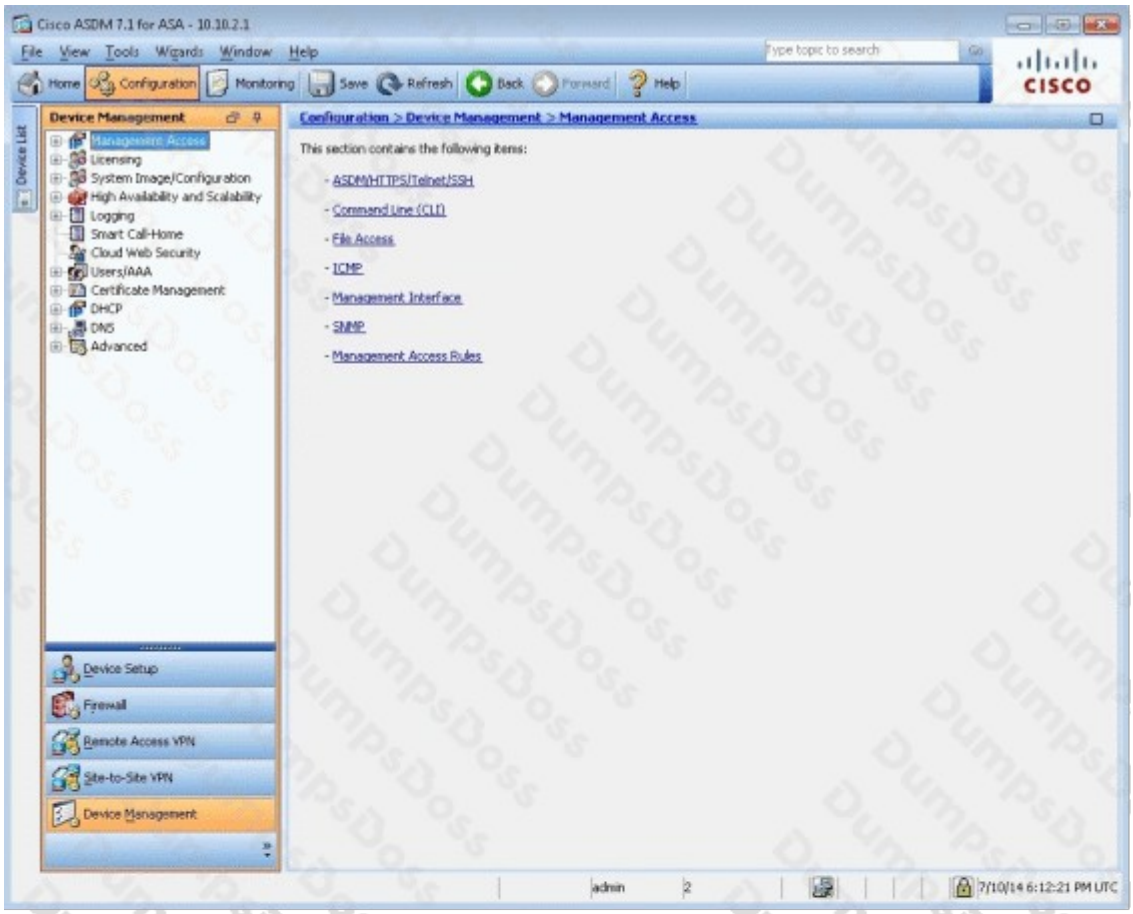

Cisco ASDM 7.1
View Tools Wizards Window
Home Configuration Monitoring
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
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
Name:
Type:
Network
Advanced NAT Settings
Translate DNS replies for rule
Interface
Source Interface:
--Any--
Destination Interface:
--Any--
DMZ
Guest
Site-to-Site
inside
managment
outside
OK
Cancel
Help
Translate TCP and UDP ports into flat range 1024-65535
Include range 1-1023
Fall through to interface PAT(dest intf):
DMZ
Use IPv6 for interface PAT
Advanced
OK
Cancel
Help
Object NAT Address
ObjectNATAddress
Scenario
TOPOLOGY

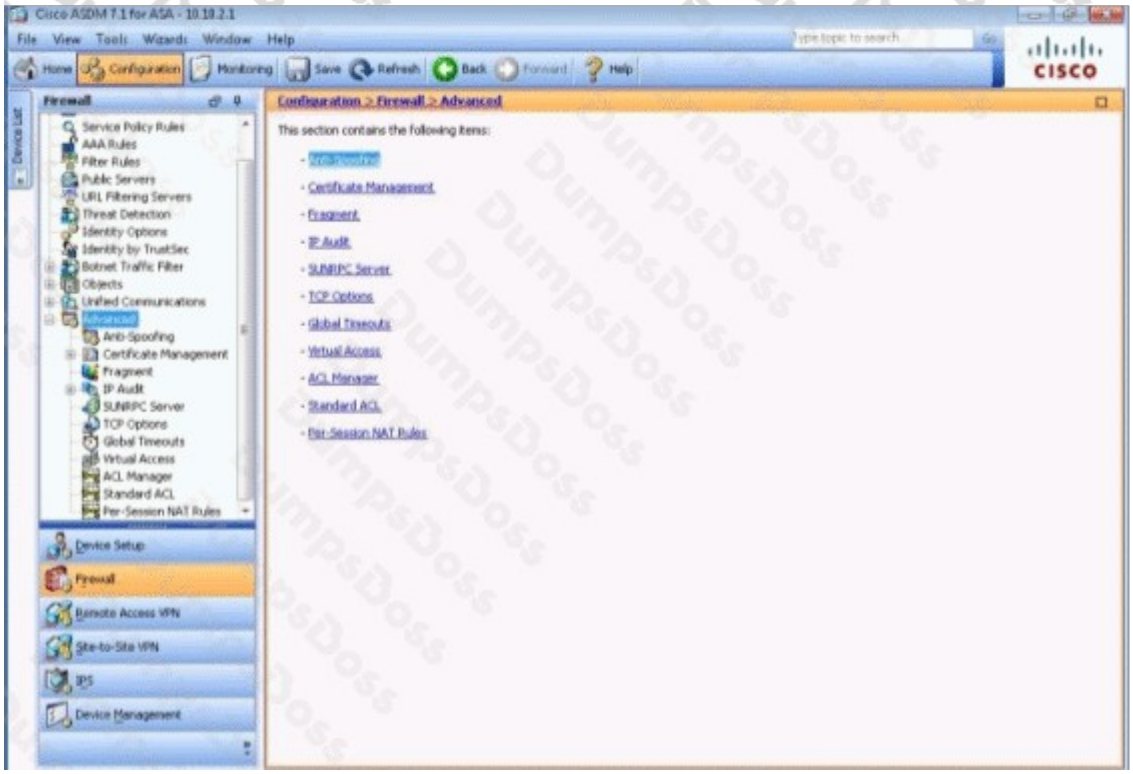

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Match Criteria: Original Packet
Action: Translated Packet
Source Intf
Dest Intf
Source
Destination
Service
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Apply
Reset


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
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
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Match Criteria: Original Packet
Action: Translated Packet
Source Intf
Dest Intf
Source
Destination
Service
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Apply
Reset

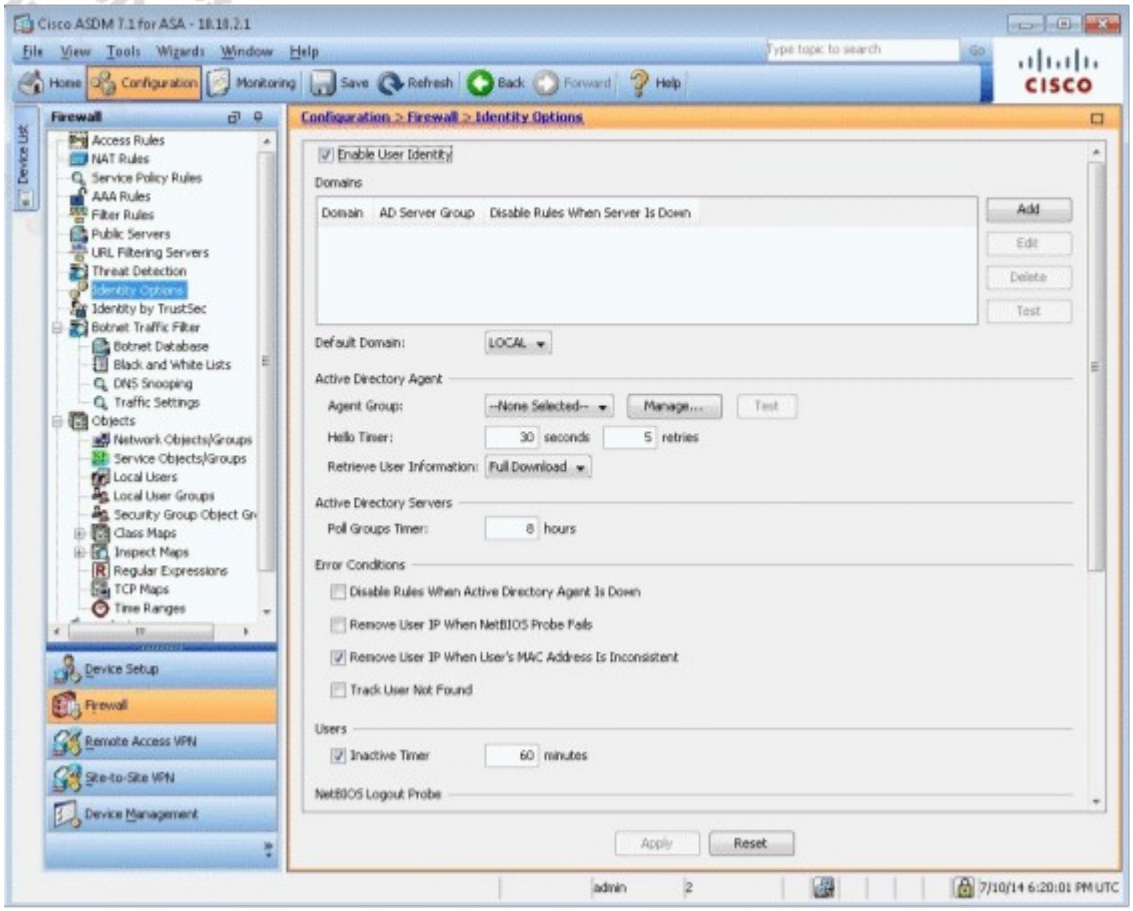

Edit NAT Rule

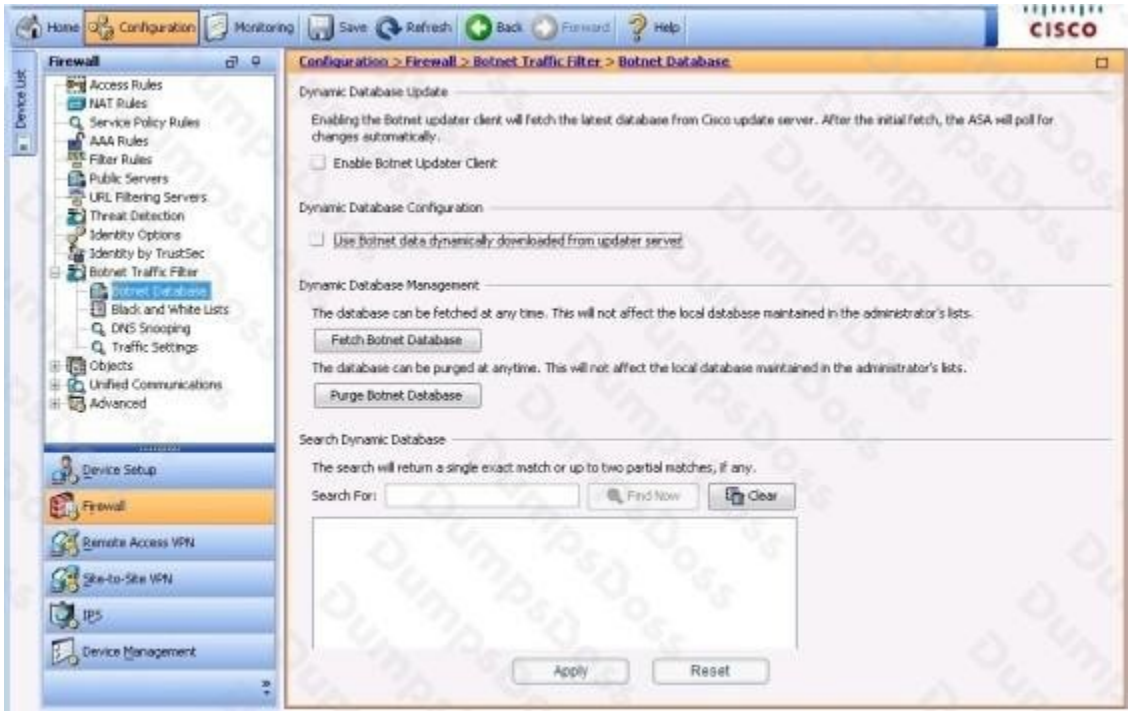

Edit NAT Rule
Match Criteria: Original Packet
Source Interface:
inside
Destination Interface:
outside
Source Address:
any
Destination Address:
any
Service:
any
Action: Translated Packet
Source NAT Type:
Dynamic
Source Address:
outside-nat-pool
Destination Address:
-- Original --
Use one-to-one address translation
PAT Pool Translated Address:
Service:
-- Original --
Round Robin
Extend PAT uniqueness to per destination instead of per interface
Translate TCP and UDP ports into flat range 1024-65535
Include range 1-1023
Fall through to interface PAT
Use IPv6 for source interface PAT
Use IPv6 for destination interface PAT
Options
Enable rule
Translate DNS replies that match this rule
Disable Proxy ARP on egress interface
Lookup route table to locate egress interface
Direction:
Both
Description:
OK
Cancel
Help

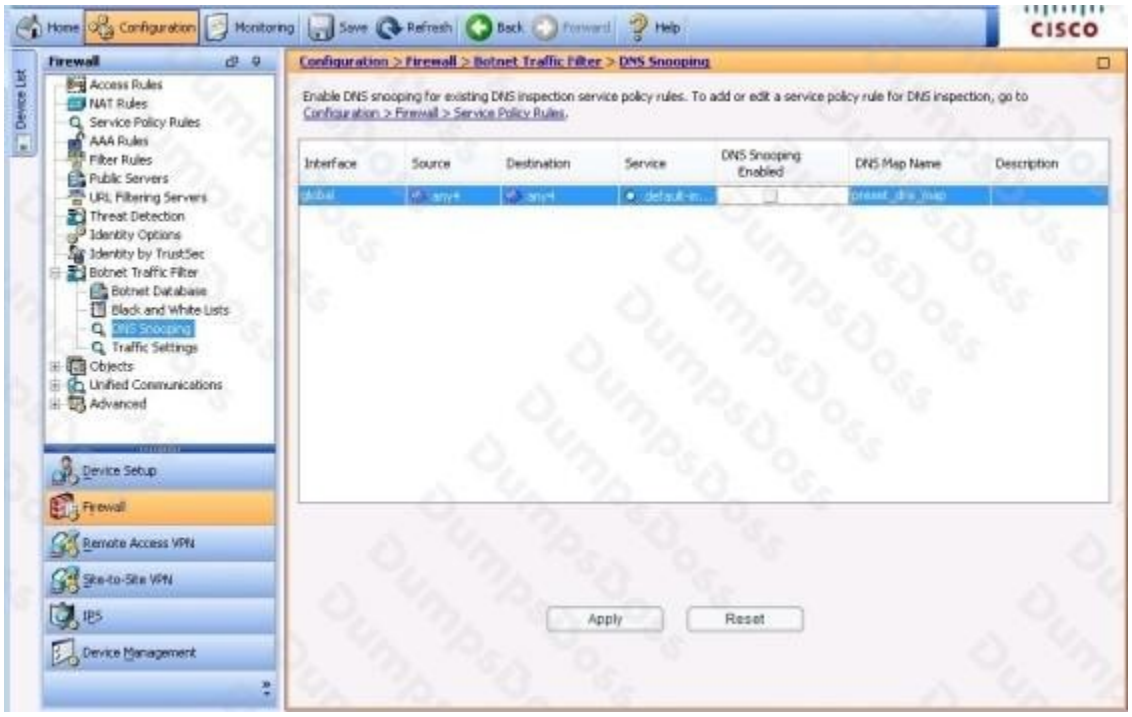

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
DHCP
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Management Access
This section contains the following items:
- ASDM/HTTPS/Telnet/SSH
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- SNMP
- Management Access Rules
admin
2
7/10/14 6:12:21 PM UTC

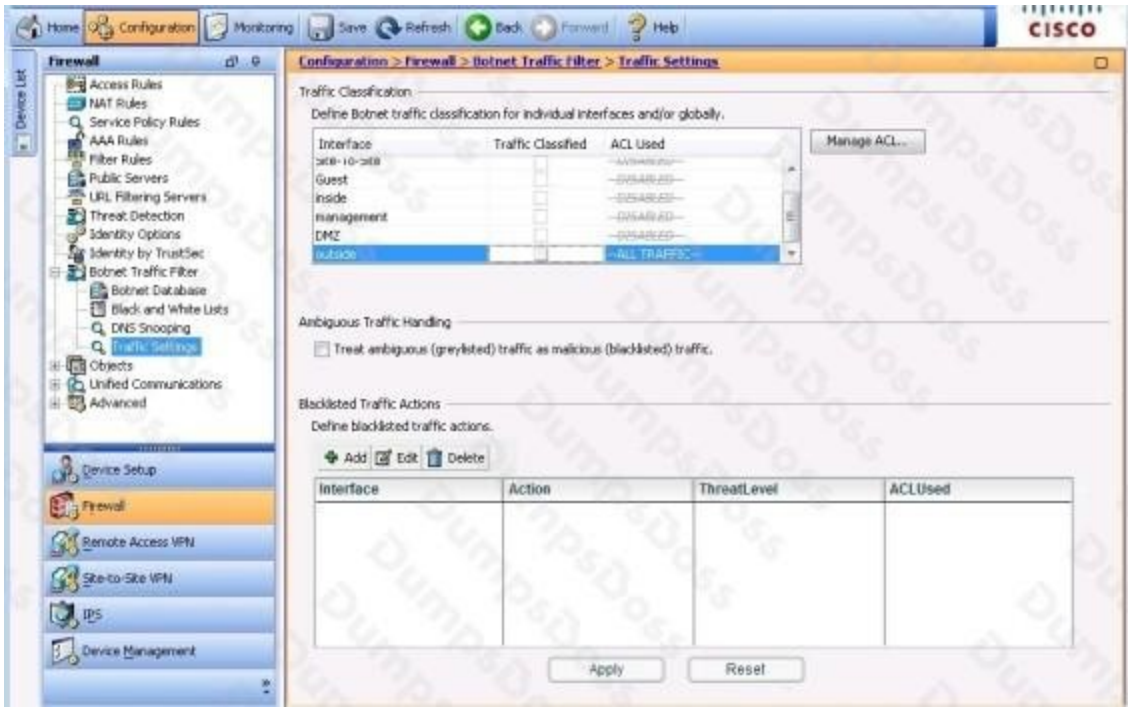

Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Anti-Spoofing
Certificate Management
Fragment
IP Audit
SUNRPC Server
TCP Options
Global Timeouts
Virtual Access
ACL Manager
Standard ACL
Per-Session NAT Rules
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Advanced
This section contains the following items:
- Anti-Spoofing
- Certificate Management
- Fragment
- IP Audit
- SUNRPC Server
- TCP Options
- Global Timeouts
- Virtual Access
- ACL Manager
- Standard ACL
- Per-Session NAT Rules

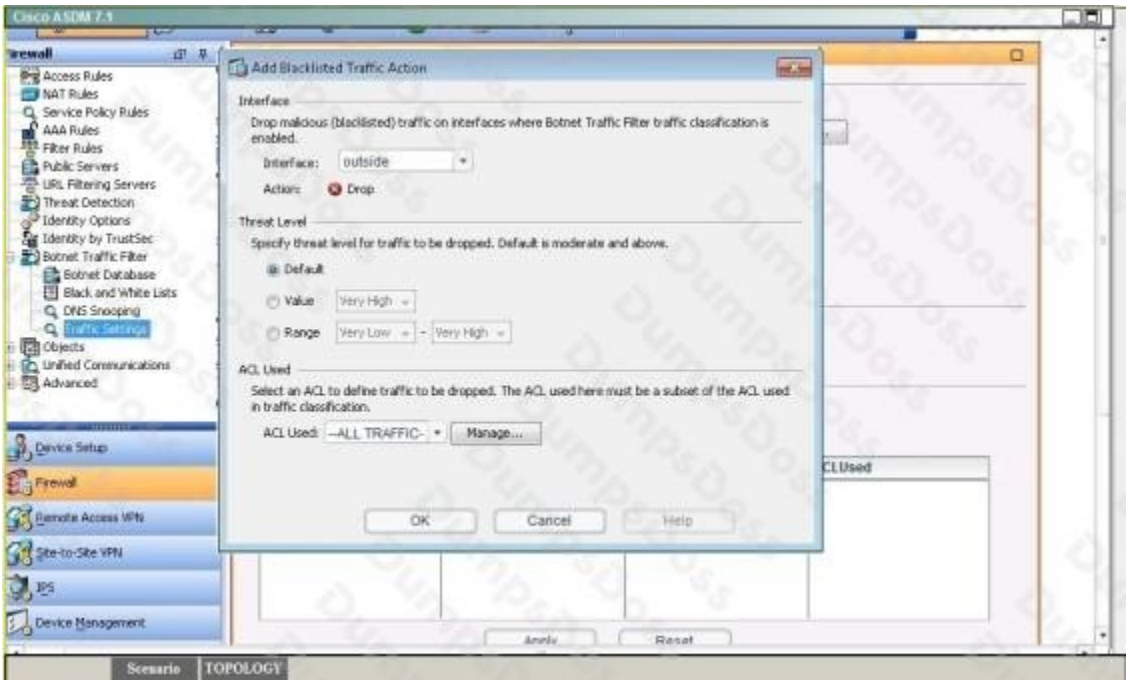

IPS
Device Management
admin
15
5/14/14 6:05:08 PM GMT


Cisco ASDM 7.1 for ASA - 18.18.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Identity Options
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
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Enable User Identity
Domains
Domain AD Server Group Disable Rules When Server Is Down
Add
Edit
Delete
Test
Default Domain: LOCAL
Active Directory Agent
Agent Group: --None Selected-- Manage... Test
Hello Timer: 30 seconds 5 retries
Retrieve User Information: Full Download
Active Directory Servers
Poll Groups Timer: 8 hours
Error Conditions
Disable Rules When Active Directory Agent Is Down
Remove User IP When NetBIOS Probe Fails
Remove User IP When User's MAC Address Is Inconsistent
Track User Not Found
Users
Inactive Timer 60 minutes
NetBIOS Logout Probe
Apply
Reset
admin
2
7/10/14 6:20:01 PM UTC


Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Botnet Traffic Filter > Botnet Database
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
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Dynamic Database Update
Enabling the Botnet updater client will fetch the latest database from Cisco update server. After the initial fetch, the ASA will poll for changes automatically.
Enable Botnet Updater Client
Dynamic Database Configuration
Use Botnet data dynamically downloaded from updater server
Dynamic Database Management
The database can be fetched at any time. This will not affect the local database maintained in the administrator's lists.
Fetch Botnet Database
The database can be purged at anytime. This will not affect the local database maintained in the administrator's lists.
Purge Botnet Database
Search Dynamic Database
The search will return a single exact match or up to two partial matches, if any.
Search For:
Find Now
Clear
Apply
Reset


Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
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
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Botnet Traffic Filter > DNS Snooping
Enable DNS snooping for existing DNS inspection service policy rules. To add or edit a service policy rule for DNS inspection, go to Configuration > Firewall > Service Policy Rules.
Interface
Source
Destination
Service
DNS Snooping Enabled
DNS Map Name
Description
Apply
Reset


Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
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
Botnet Database
Black and White Lists
DNS Snooping
Traffic Settings
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Firewall > Botnet Traffic Filter > Traffic Settings
Traffic Classification
Define Botnet traffic classification for individual interfaces and/or globally.
Interface
Traffic Classified
ACL Used
Manage ACL...
Guest
inside
management
DMZ
outside
Ambiguous Traffic Handling
Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic.
Blacklisted Traffic Actions
Define blacklisted traffic actions.
Add
Edit
Delete
Interface
Action
ThreatLevel
ACLUsed
Apply
Reset



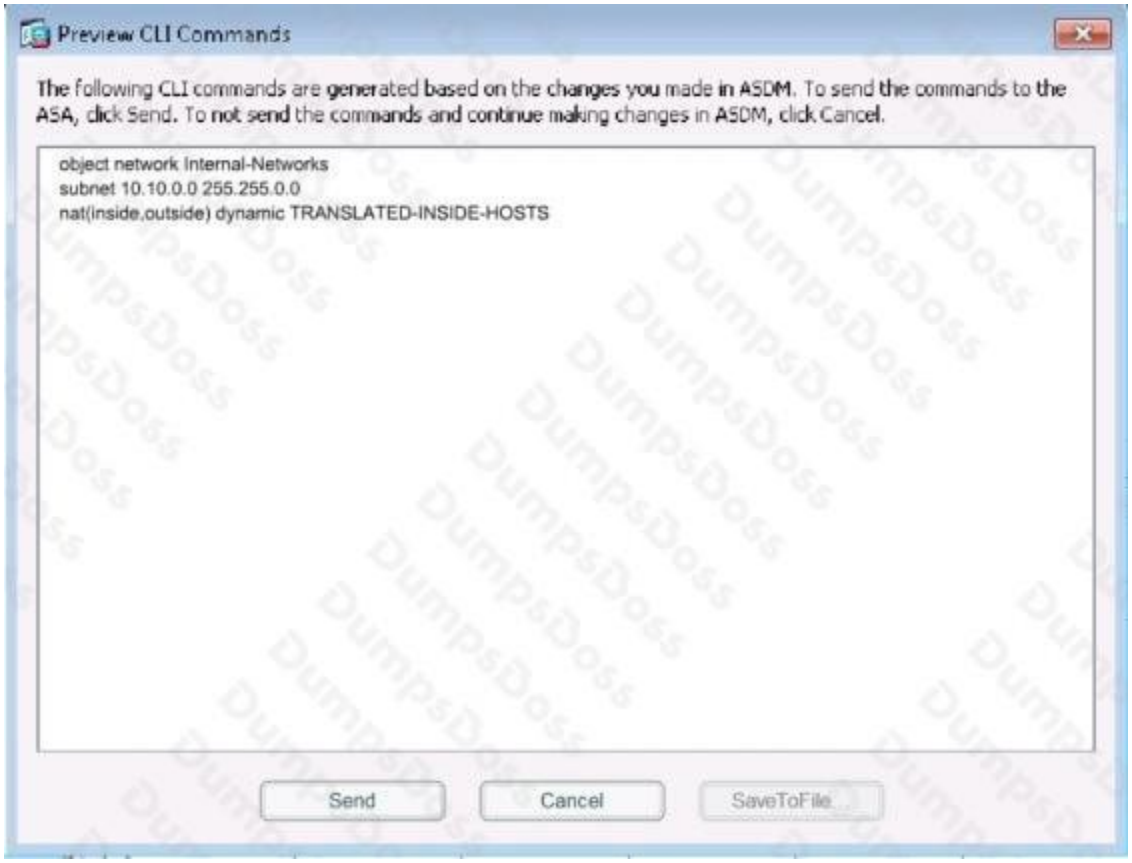
ANSWER: Review the explanation for detailed answer steps.

Explanation:

First, click on Configuration ->Site-to-Site VPN to bring up this screen:

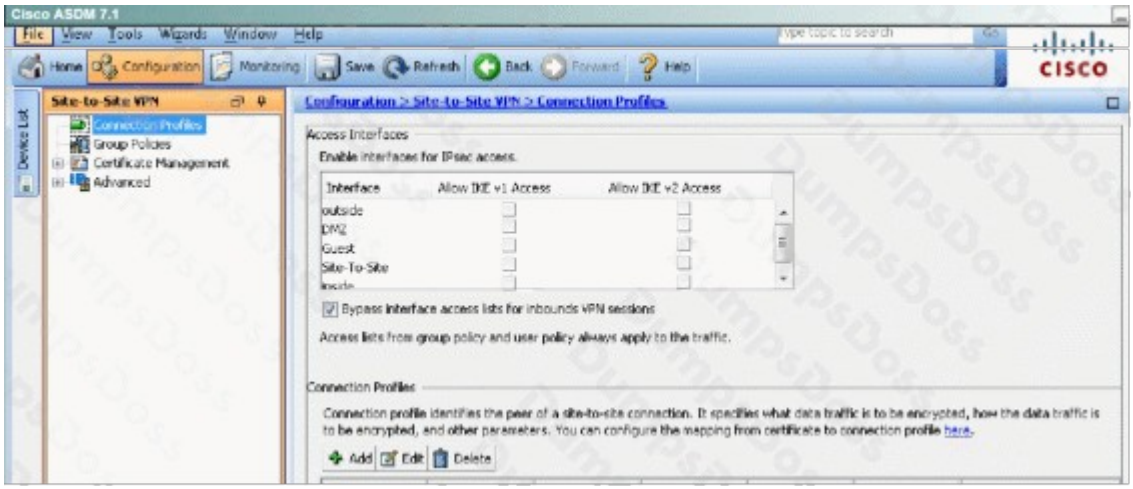
Click on “allow IKE v1 Access” for the outside per the instructions as shown below:

Then click apply at the bottom of the page. This will bring up the following pop up message:

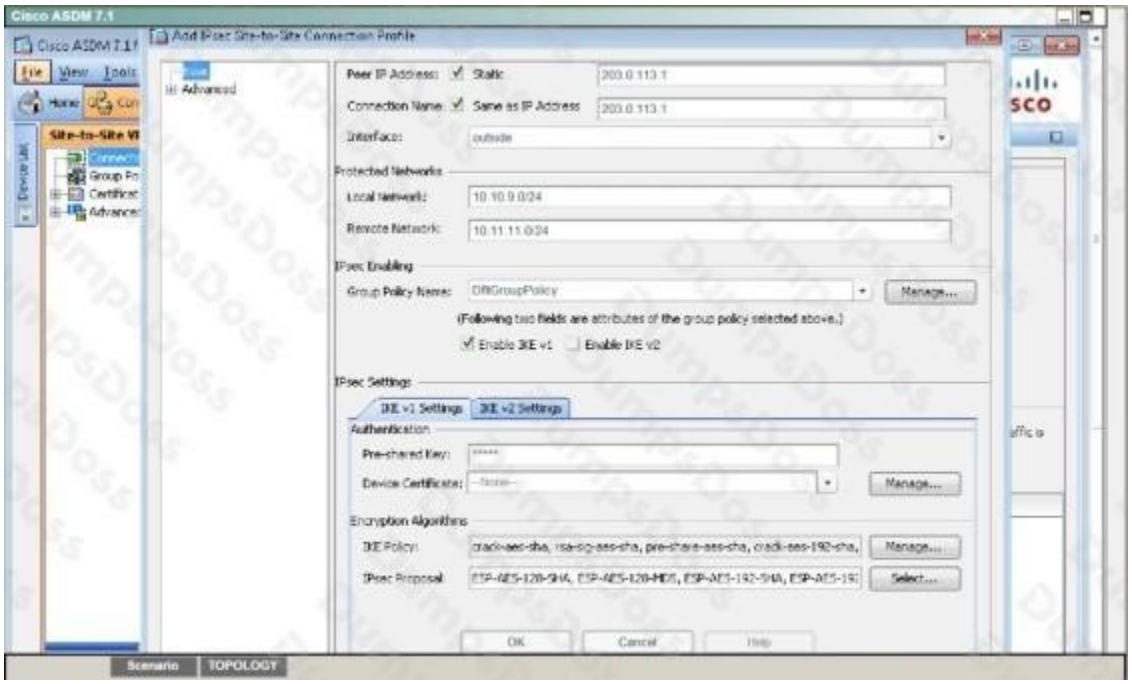


Click on Send.

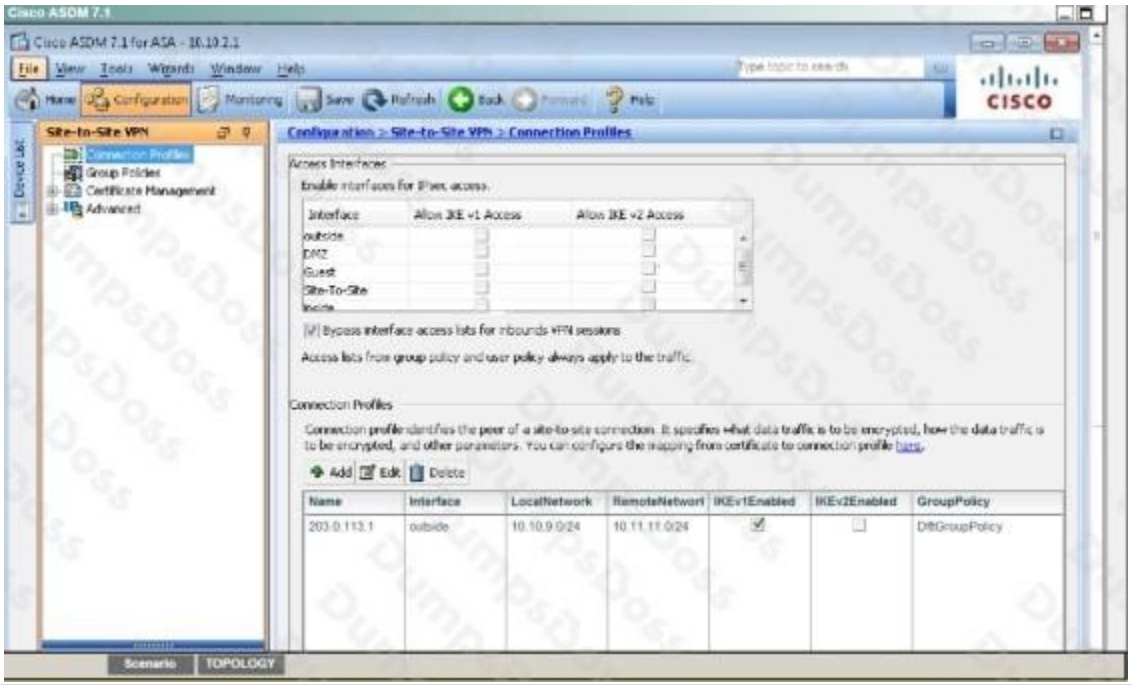
Next, we need to set up the connection profile. From the connection profile tab, click on “Add”



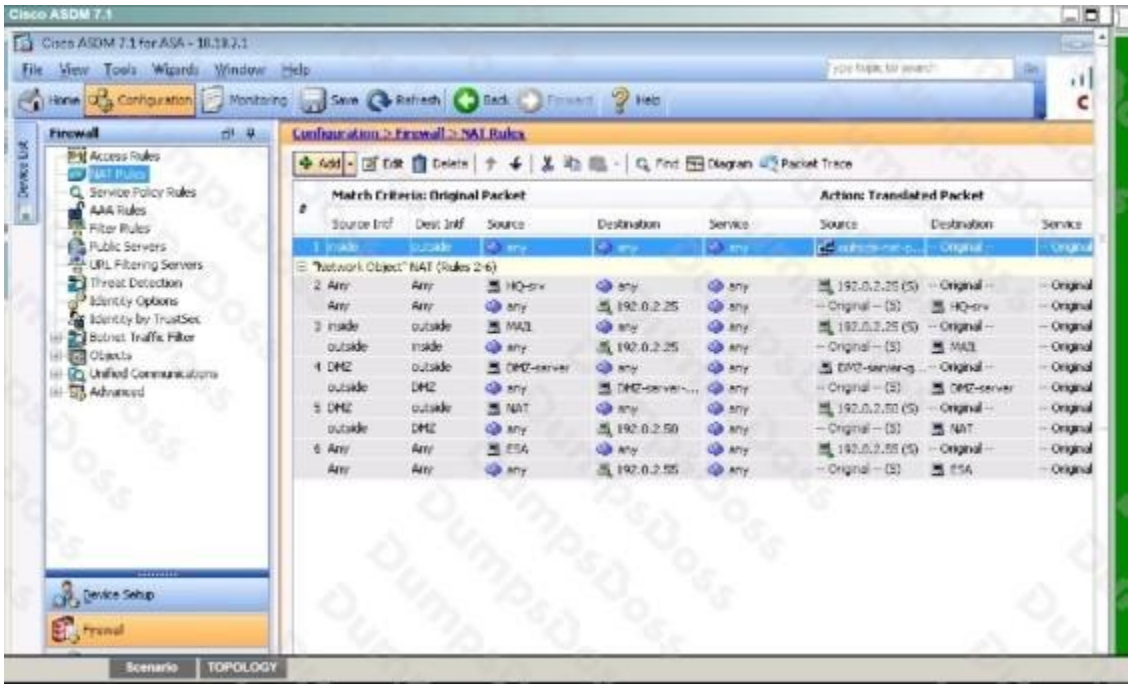
Then, fill in the information per the instructions as shown below:



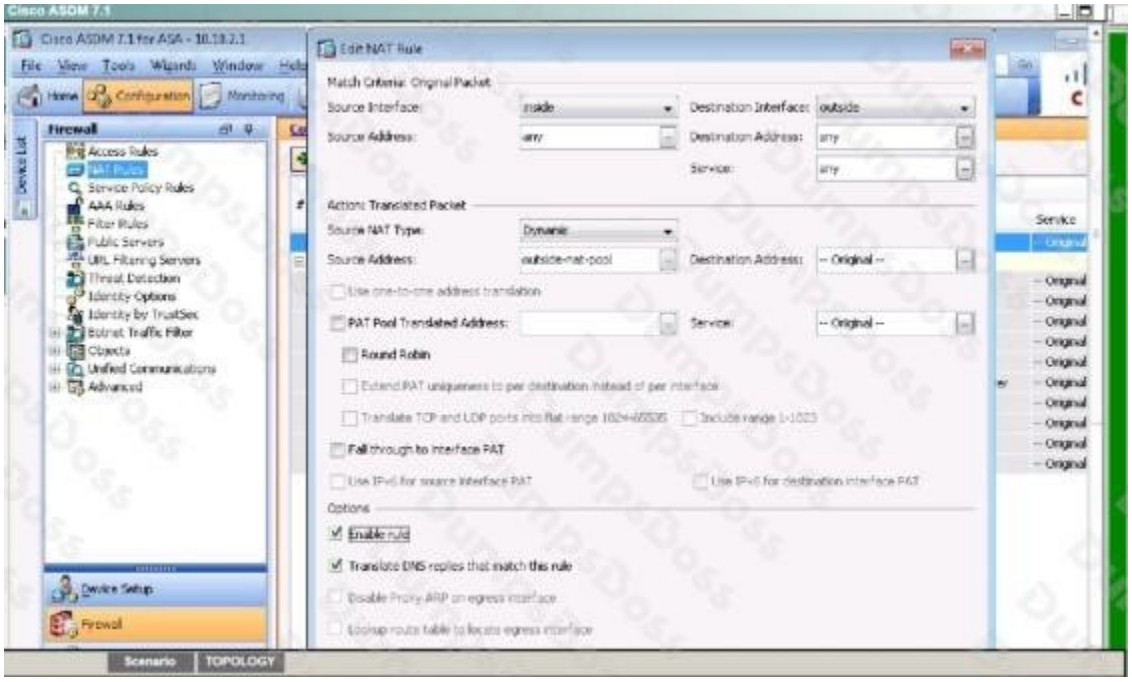
Hit OK and you should see this:



To test this, we need to disable NAT. Go to Configuration -> Firewall -> NAT rules and you should see this:

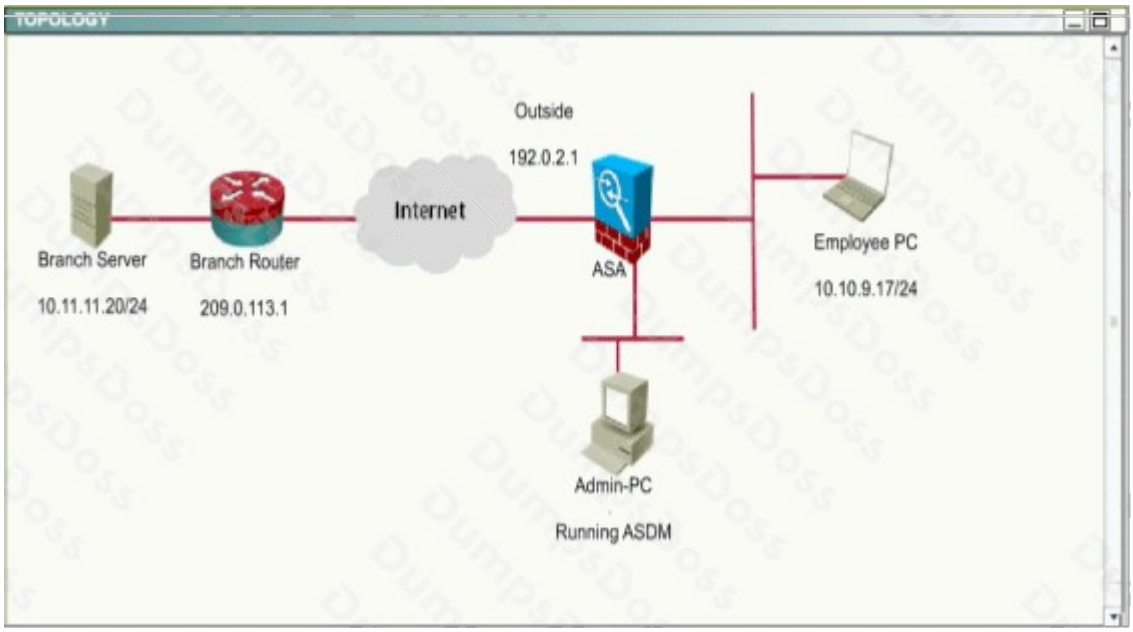


Click on Rule 1 to get the details and you will see this:



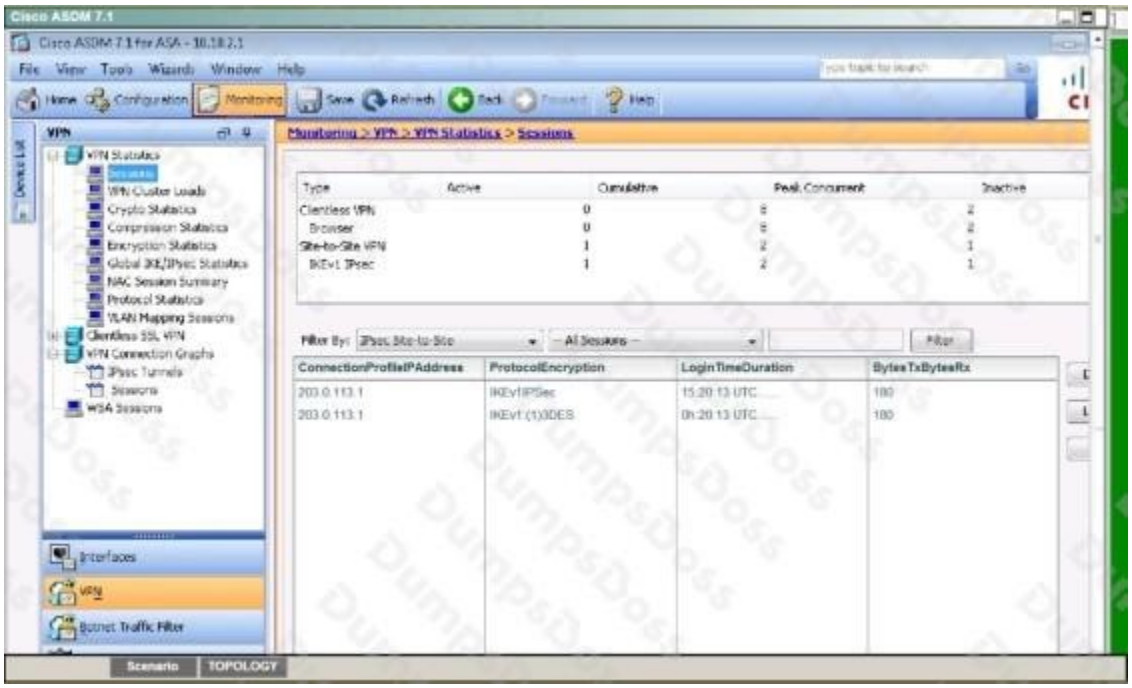
We need to uncheck the “Enable rule” button on the bottom. It might also be a good idea to uncheck the “Translate DNS replies that match the rule” but it should not be needed.

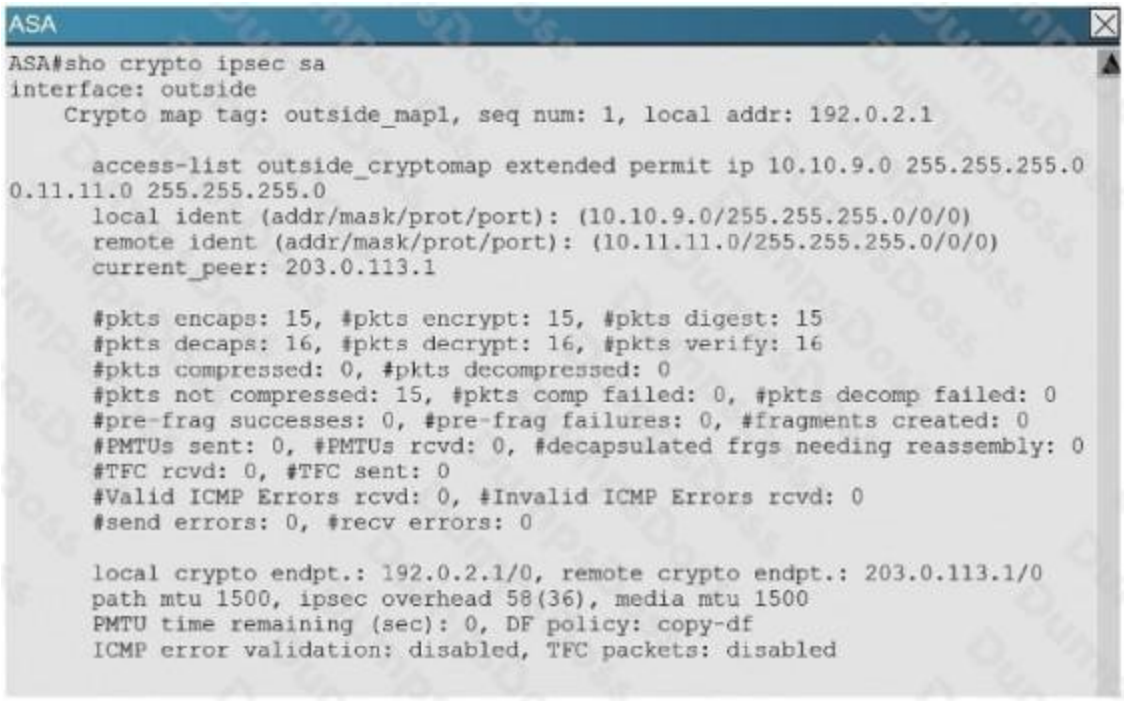
Then, go back to the topology:



Click on Employee PC, and you will see a desktop with a command prompt shortcut. Use this to ping the IP address of 10.11.11.20 and you should see replies:

We can also verify by viewing the VPN Statistics -> Sessions and see the bytes in/out incrementing as shown below:





QUESTION NO: 18

Which three configurations are required for both IPsec VTI and crypto map-based VPNs?

(Choose three.)

A. transform set

B. ISAKMP policy

C. ACL that defines traffic to encrypt

D. dynamic routing protocol

E. tunnel interface

F. IPsec profile

G. PSK or PKI trustpoint with certificate

ANSWER: A B G

QUESTION NO: 19

Which Cisco IOS feature provides secure, on-demand meshed connectivity?

A. Easy VPN

B. IPsec VPN

C. mGRE

D. DMVPN

ANSWER: D