Cisco

Exam 300-209

Implementing Cisco Secure Mobility Solutions

Version: 10.0

[Total Questions: 213]

Question No : 1

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 : 2

Which of the following could be used to configure remote access VPN Host-scan and pre-login policies?

A. ASDM
B. Connection-profile CLI command
C. Host-scan CLI command under the VPN group policy
D. Pre-login-check CLI command

Answer: A

Question No : 3

Which four activities does the Key Server perform in a GETVPN deployment? (Choose four.)

A. authenticates group members
B. manages security policy
C. creates group keys
D. distributes policy/keys
E. encrypts endpoint traffic
F. receives policy/keys
G. defines group members

Answer: A,B,C,D

Question No : 4

A user is unable to establish an AnyConnect VPN connection to an ASA. When using the Real-Time Log viewer within ASDM to troubleshoot the issue, which two filter options would the administrator choose to show only syslog messages relevant to the VPN connection? (Choose two.)

A. Client's public IP address
B. Client's operating system
C. Client's default gateway IP address
D. Client's username
E. ASA's public IP address

Answer: A,D

Question No : 5

The Cisco AnyConnect client is unable to download an updated user profile from the ASA headend using IKEv2. What is the most likely cause of this problem?

A. User profile updates are not allowed with IKEv2.
B. IKEv2 is not enabled on the group policy.
C. A new profile must be created so that the adaptive security appliance can push it to the client on the next connection attempt.
D. Client Services is not enabled on the adaptive security appliance.

Answer: C

Question No : 6

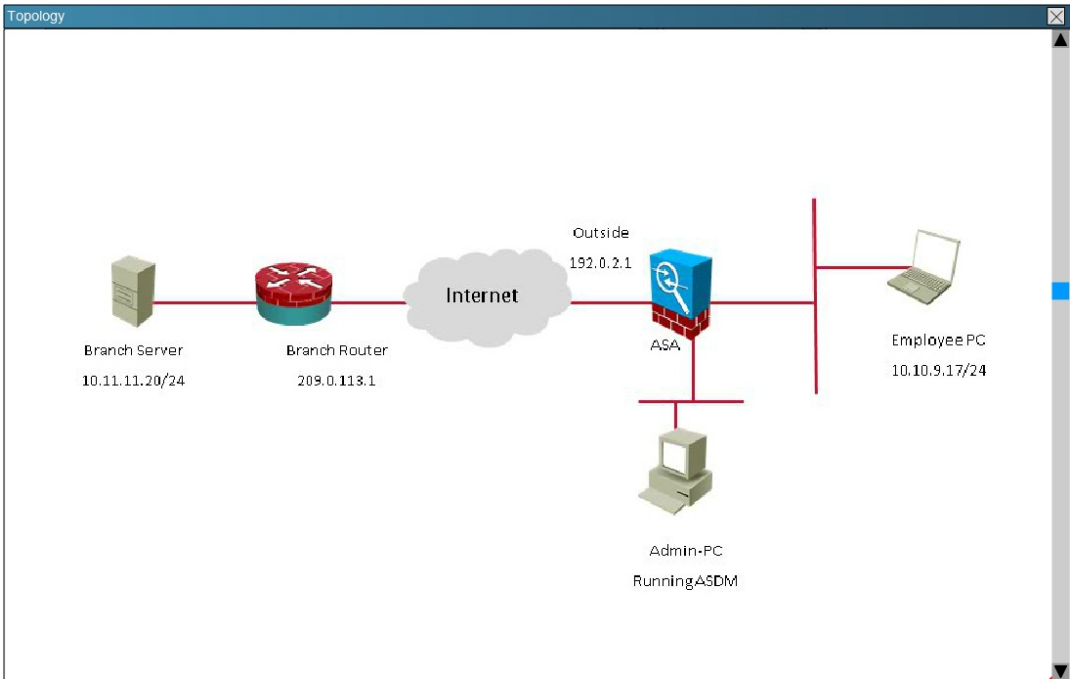
Scenario:

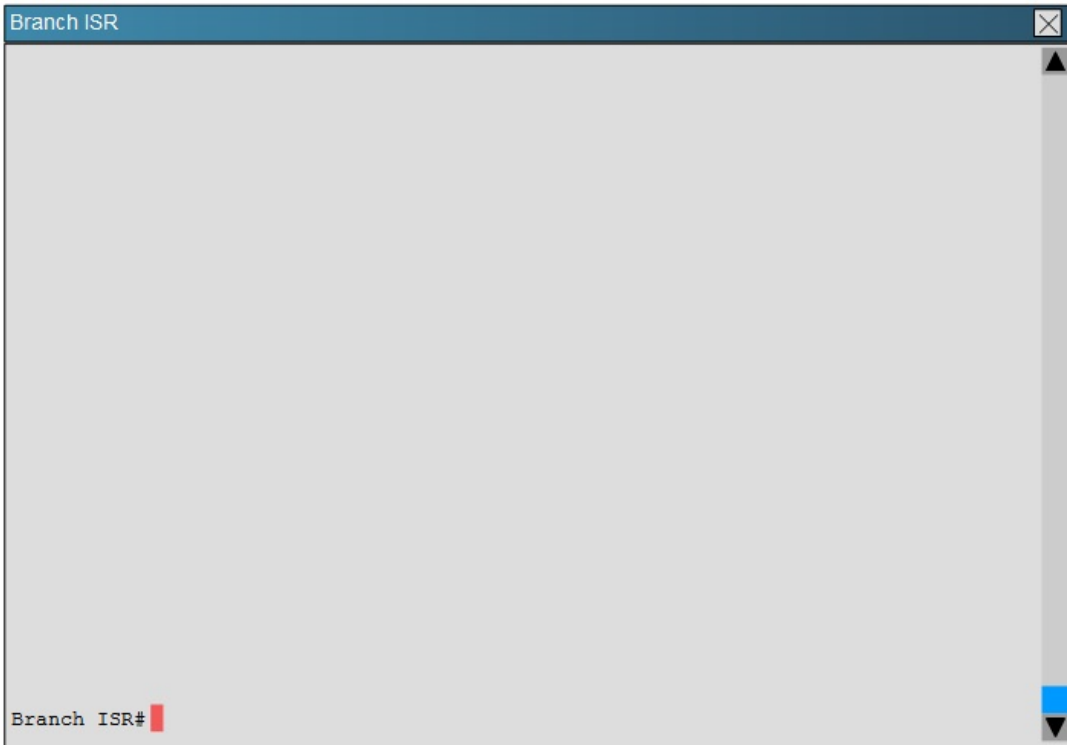
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

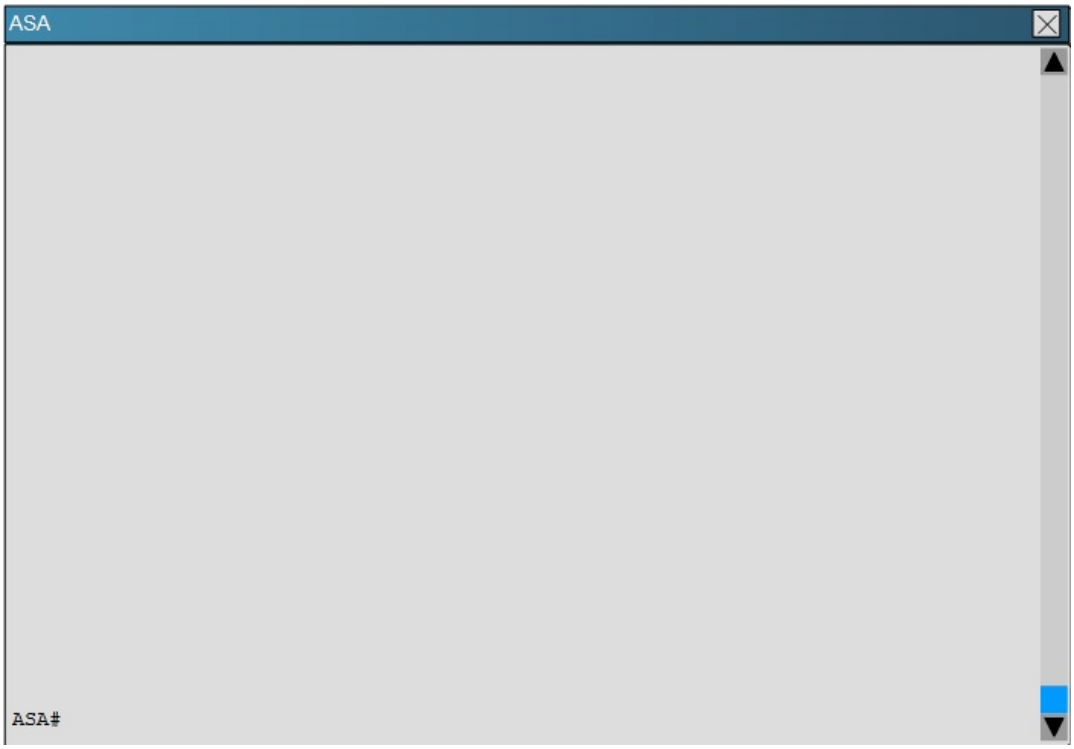
You are now tasked with verifying the IKEvl IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

NOTE: the show running-config command cannot be used for this exercise.

Topology:







Which transform set is being used on the branch ISR?

A. Default
B. ESP-3DES ESP-SHA-HMAC
C. ESP-AES-256-MD5-TRANS mode transport
D. TSET

Answer: B

Explanation:

This can be seen from the “show crypto ipsec sa” command as shown below:

Branch ISR

```
Branch ISR#show crypto ipsec sa
interface: GigabitEthernet0/1
    Crypto map tag: VPN-to-ASA, local addr 203.0.113.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
   current_peer 192.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
    #pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x8E47598C(2387040652)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xCE89192A(3465091370)
        transform: esp-3des esp-sha-hmac ,
```

Branch ISR

```
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
   current_peer 192.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
    #pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x8E47598C(2387040652)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xCE89192A(3465091370)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
Branch ISR#
Branch ISR#
```

Question No : 7

Which three commands are included in the command show dmvpn detail? (Choose three.)

A. show ip nhrp nhs
B. show dmvpn
C. show crypto session detail
D. show crypto ipsec sa detail
E. show crypto sockets
F. show ip nhrp

Answer: A,B,C

Question No : 8

A network is configured to allow clientless access to resources inside the network. Which feature must be enabled and configured to allow SSH applications to respond on the specified port 8889?

A. auto applet download
B. port forwarding
C. web-type ACL
D. HTTP proxy

Answer: B

Question No : 9

Scenario

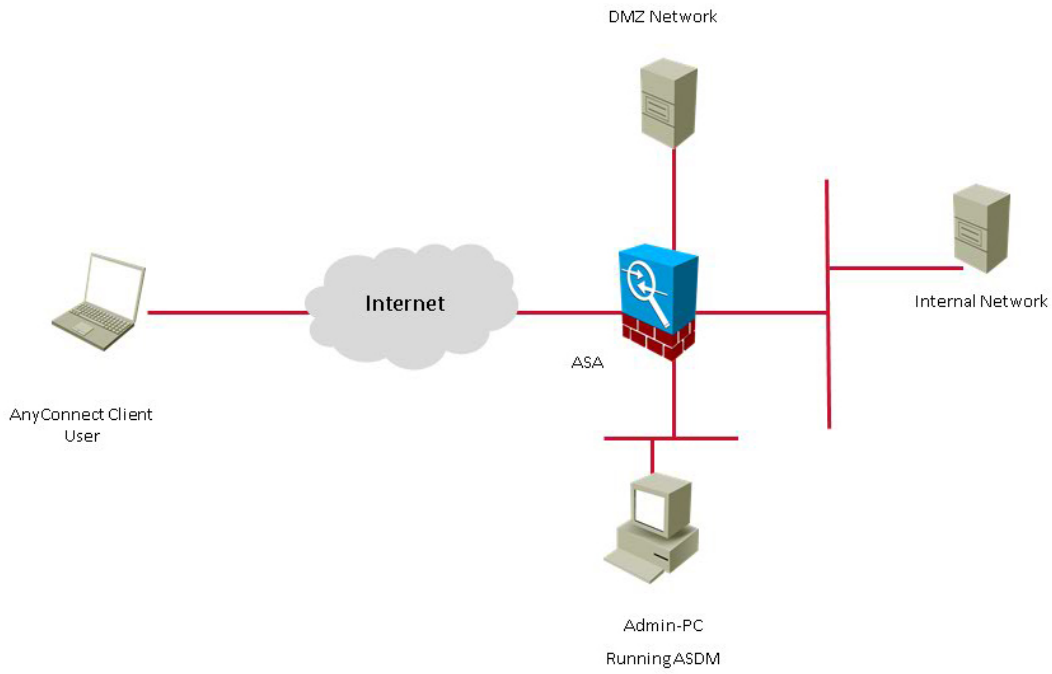
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

Note: Not all screens or option selections are active for this exercise.

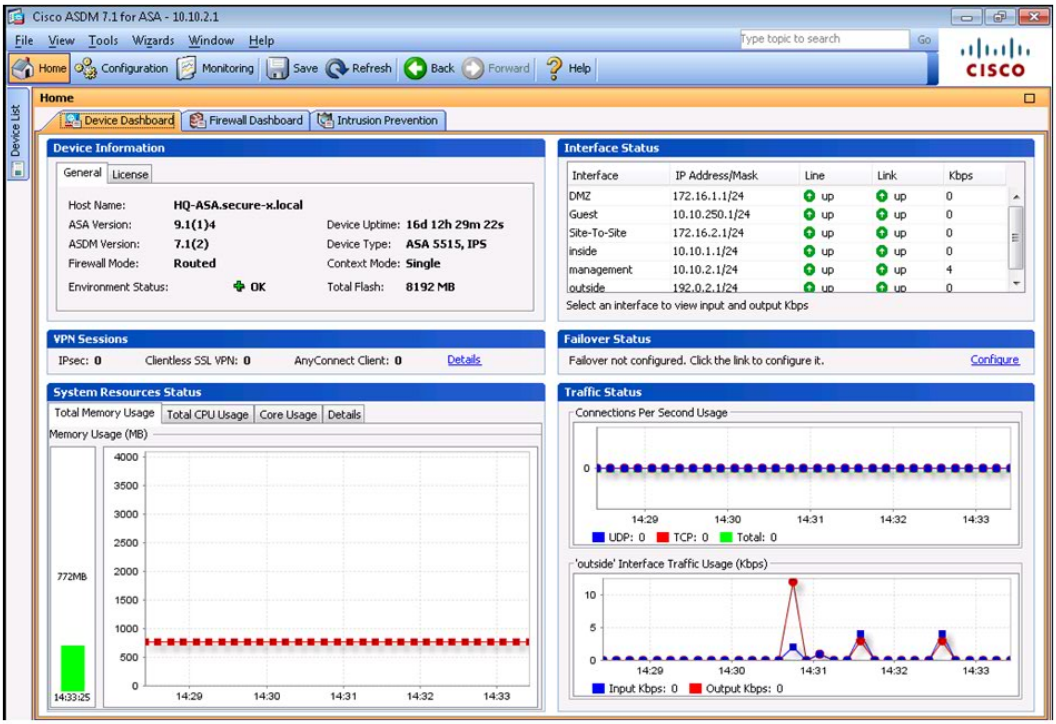
Instructions

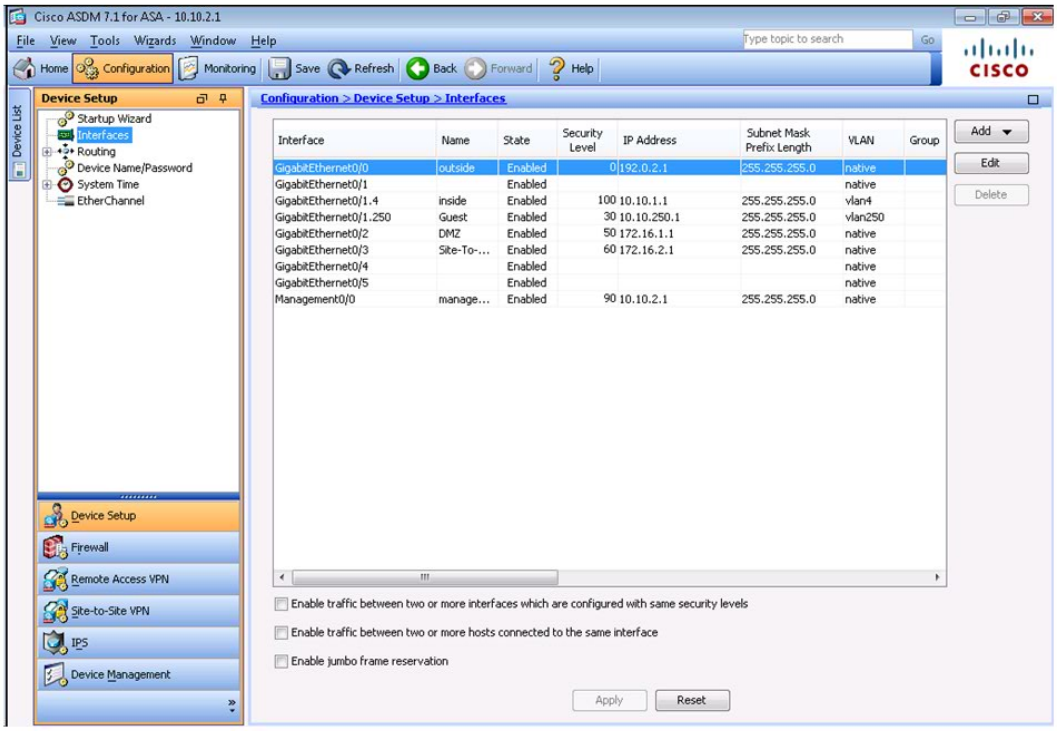
- Naviagate the ASDM GUI on the device to verify network operation and answer for multiple-choice questions.
- You may have to use the scoll bars to view the entire ASDM Configuration screens.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- **NOT ALL SCREENS AND SELECTIONS ARE AVAILABLE FOR THIS EXERCISE.**
- Click on the Admin PC on the topology page to gain ASDM to the ASA. No passwords are required for this exercise.
- You may also click on the Default Home tab to access ASDM or return to the ASDM home screen at any time.
- There are **four (4)** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.
- To access the multiple-choice questions, click on the Questions tab and then numbered boxes on the left of the panel to view each question.

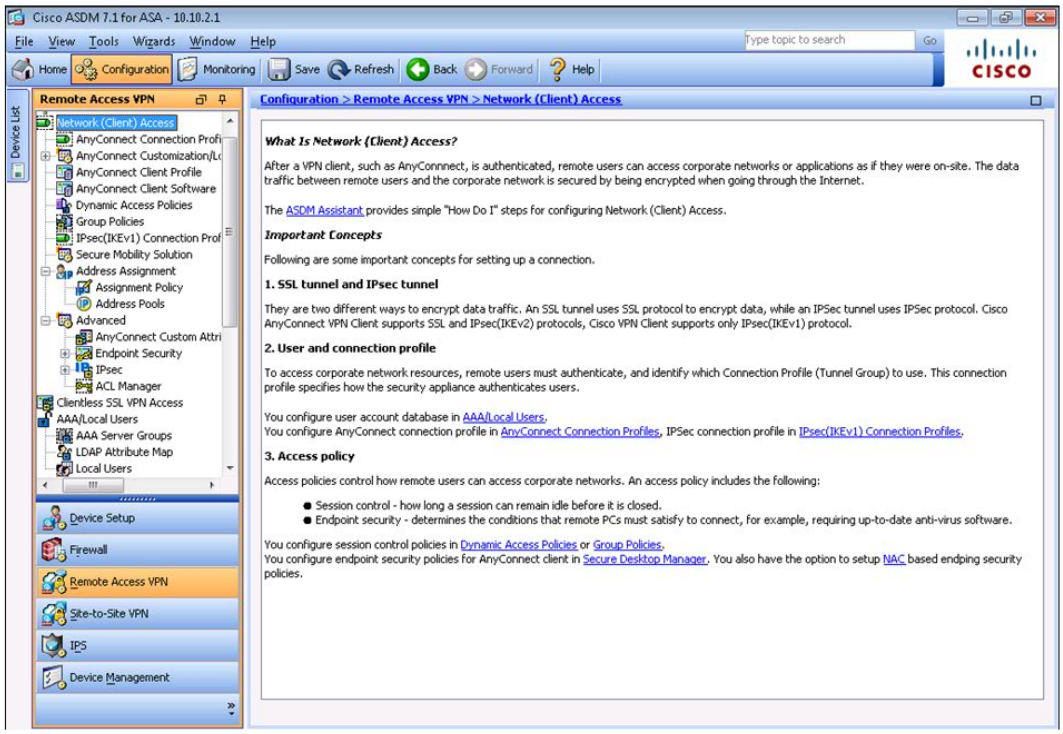
Topology

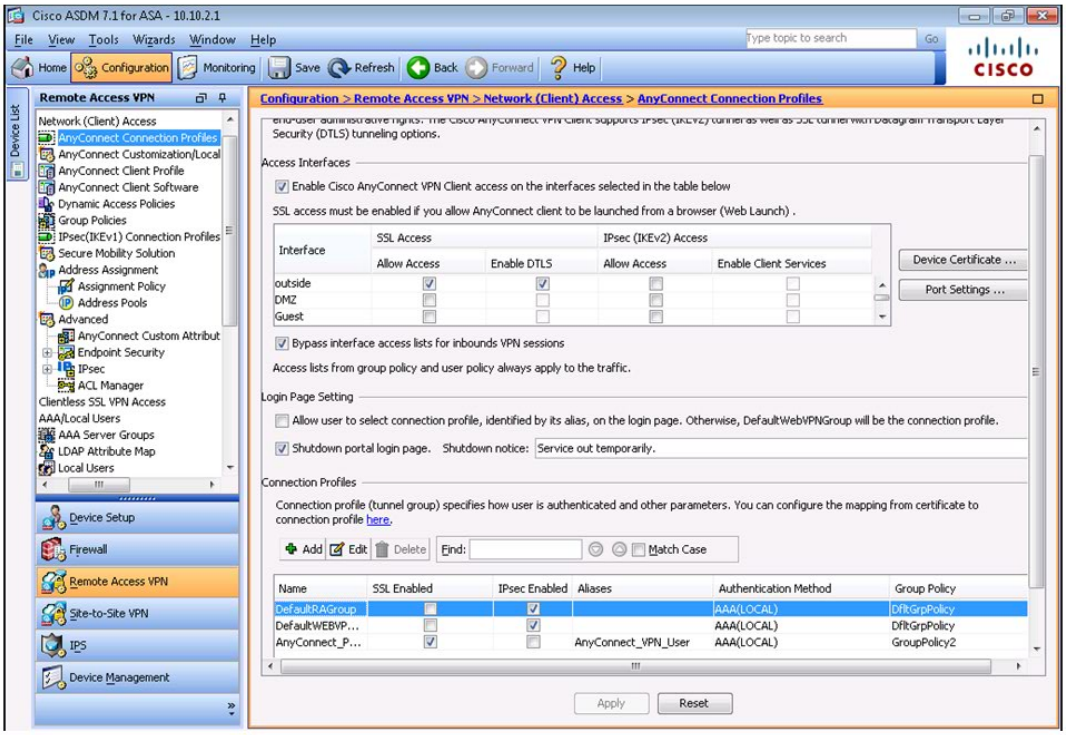


Default_Home


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Home
Device Dashboard Firewall Dashboard Intrusion Prevention
Device Information
General License
Host Name: HQ-ASA.secure-x.local
ASA Version: 9.1(1)4
ASDM Version: 7.1(2)
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 16d 12h 29m 22s
Device Type: ASA 5515, IPS
Context Mode: Single
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)
772MB
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
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 0 192.0.2.1 255.255.255.0 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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
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


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
Network (Client) Access
AnyConnect Connection Profi
AnyConnect Customization/Lo
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Prof
Secure Mobility Solution
Address Assignment
Assignment Policy
Address Pools
Advanced
AnyConnect Custom Attri
Endpoint Security
IPsec
ACL Manager
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
What Is Network (Client) Access?
After a VPN client, such as AnyConnnect, 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 ASDM 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
They 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 endping security policies.


Cisco ASDM 7.1 for ASA - 10.10.2.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Local
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Assignment Policy
Address Pools
Advanced
AnyConnect Custom Attribut
Endpoint Security
IPsec
ACL Manager
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Security (DTLS) tunneling options.
Access Interfaces
Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .
Interface
SSL Access
IPsec (IKEv2) Access
Allow Access
Enable DTLS
Allow Access
Enable Client Services
outside
DMZ
Guest
Device Certificate ...
Port Settings ...
Bypass interface access lists for inbounds VPN sessions
Access lists from group policy and user policy always apply to the traffic.
Login Page Setting
Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.
Shutdown portal login page.
Shutdown notice:
Service out temporarily.
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.
Add
Edit
Delete
Find:
Match Case
Name
SSL Enabled
IPsec Enabled
Aliases
Authentication Method
Group Policy
DefaultRAGroup
AAA(LOCAL)
DfltGrpPolicy
DefaultWEBVP...
AAA(LOCAL)
DfltGrpPolicy
AnyConnect_P...
AnyConnect_VPN_User
AAA(LOCAL)
GroupPolicy2
Apply
Reset