**Layer 3 security using web based clientless vpn**

A Project Submitted

in Partial Fulfillment of the Requirements

for the Degree of

# Bachelor In Technology

in

# Information Technology

by

# Vikrant Singh , Ustam saini

To

Ms.Ritika Arora

Information Technology

FACULTY OF ENGINEERING AND TECHNOLOGY

UIET HOSHIARPUR,INDIA

# **November,2019**

**Contents**

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Configuration**

**Future Scope**

**References**

**ABSTRACT**

Information is now a vital part of our economy and our society, from the millions of digital transactions happening daily to our personal tax and medical records. And just as we use armored protection and security vaults to protect valuable assets, network security is the protector of that information.

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.

Who needs network security?

Why don't we just build encryption and anti malware protection into end-points and simply enjoy open networks? From a security perspective that's always best and it's in line with the vision. But in the real world it's not so simple.

At the very least we need protective measures in networks to guarantee availability and performance. Beyond that there is huge potential to deliver value through security features in networks.

In fact there has always been more to network security than users realize. Fallback, monitoring and filtering are ever-present but invisible to endpoints. Many application owners believe their systems operate on top of a pure IP infrastructure, but nothing could be further from the truth -- enterprise networks are heavily structured.

The future of network security might be far from clear-cut. One thing is clear - it will certainly be richer and more sophisticated than we've seen so far. Determining how to plan for a business environment in which everyone is connected and security expectations are high is not trivial. We all have to do it.

**Introduction**

There has been tremendous growth in past few year, regarding cyber crimbe , which leads an organization loose millions over night. So, not high but we have to implement basic security in our network and one of the way is to protect layer 3 of our OSI model, using VPN. There are several VPN's available in the market like IPsec, SSL VPN . So, we implement basic layer 3 security using clientless VPN service and verification using ftp access and wireshark monitoring over the links.

**Prerequisites**

**Requirements**

There are no specific requirements for this document.

**Components Used**

The information in this document is based on these software and hardware versions:

* CISCO ASA 5505.
* Clientless VPN.
* WIRESHARK.
* VIRTUAL BOX.
* QEMU.
* ROUTER IOS 7200.
* GNS3 OFFLINE VERSION FOR SIMULATION.

**1. CISCO ASA 5505 :**The Cisco ASA 5505 is a full-featured firewall for small business, branch, and enterprise teleworker environments. It delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, immediately operational appliance. Using the integrated graphical Cisco Adaptive Security Device Manager (ASDM), the Cisco ASA 5505 can be rapidly deployed and easily managed, helping businesses reduce operational costs. It features a flexible 8-port 10/100 Fast Ethernet switch whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for improved network segmentation and security.

The Cisco ASA 5505 provides two Power over Ethernet (PoE) ports, simplifying the deployment of Cisco IP phones with highly secure zero-touch voice over IP (VoIP) capabilities and the deployment of external wireless access points for extended network mobility. A high-performance intrusion prevention and worm mitigation service is available with the addition of the Advanced Inspection and Prevention Security Services Card (AIP SSC). Multiple USB ports can be used to implement additional services and capabilities, as needed.

As your business needs grow, you can install a Security Plus upgrade license, The Cisco ASA 5505 can then scale to support a higher site to site VPN connection capacity of 25 IPsec VPN connections, add full DMZ support, and integrate into switched network environments through VLAN trunking support. This upgrade license improves business continuity by helping to enable support for redundant ISP connections and stateless active/standby high-availability services

.

Businesses can also extend the Cisco ASA 5505’s VPN service by enabling the Cisco AnyConnect client and clientless VPN remote access to support various mobile workers and business partners. Cisco secure remote access solution deployments can scale to serve up to 25 Cisco AnyConnect or clientless VPN concurrent users on each Cisco ASA 5505. Licenses for AnyConnect are purchased separately from the ASA based on feature tier (Plus/Apex) unique/authorized user count and term. The Apex tier also supports clientless SSL VPN connectivity.

This combination of market-leading security and VPN services, advanced networking features, flexible remote management capabilities, and future extensibility makes the Cisco ASA 5505 an excellent choice for businesses requiring a best-in-class small business, branch, or enterprise teleworker security solution.

## **Introduction to Clientless SSL VPN****:** Clientless SSL VPN enables end users to securely access resources on the corporate network from anywhere using an SSL-enabled Web browser. The user first autehnticates with a Clientless SSL VPN gateway, which then allows the user to access pre-configured network resources.Clientless SSL VPN creates a secure, remote-access VPN tunnel to an ASA using a Web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of Web resources and both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTP. They include:

* Internal websites.
* Web-enabled applications.
* NT/Active Directory file shares.
* email proxies, including POP3S, IMAP4S, and SMTPS.
* Microsoft Outlook Web Access Exchange Server 2000, 2003, and 2007.
* Microsoft Web App to Exchange Server 2010 in 8.4(2) and later.
* Application Access (smart tunnel or port forwarding access to other TCP-based applications)

Clientless SSL VPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide the secure connection between remote users and specific, supported internal resources that you configure at an internal server. The ASA recognizes connections that must be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to resources by users of Clientless SSL VPN sessions on a group basis. Users have no direct access to resources on the internal network.

**3.GNS3 :**Graphical Network Simulator-3 (shortened to GNS3) is a network software emulator first released in 2008.It allows the combination of virtual and real devices, used to simulate complex networks. It uses Dynamips emulation software to simulate [Cisco IOS](https://en.wikipedia.org/wiki/Cisco_IOS) .

**4.QEMU : QEMU**(short for **Quick Emulator**) is a open source emulator that performs [hardware virtualization](https://en.wikipedia.org/wiki/Hardware_virtualization).

QEMU is a [hosted virtual machine monitor](https://en.wikipedia.org/wiki/Virtual_machine_monitor" \l "Classification): it emulates the machine's processor through dynamic binary translation and provides a set of different hardware and device models for the machine, enabling it to run a variety of [guest operating systems](https://en.wikipedia.org/wiki/Guest_operating_system). It also can be used with KVM to run virtual machines at near-native speed (by taking advantage of hardware extensions such as [Intel VT-x](https://en.wikipedia.org/wiki/X86_virtualization)). QEMU can also do emulation for user-level processes, allowing applications compiled for one architecture to run on another.

**5.Router and switches :**Cisco 7200 series routers are used and following and some specifications of 7200 series routers.   
•**WAN edge**-Award-winning quality-of-service (QoS) feature performance

•**Broadband aggregation-**Up to 16,000 Point-to-Point Protocol (PPP) sessions per chassis

•**Multiprotocol Label Switching provider edge (MPLS PE)-**Number one choice for provider edge deployment today

•**Voice/video/data integration-Time**-division multiplexer (TDM)-enabled VXR chassis and voice port adapters

•**IP-to-IP Gateway Support-**Direct IP-interconnections

•**IP Security virtual private networking (IPSec VPN)-**Scalable to 5,000 tunnels per chassis

•**High-End Customer Premises Equipment (CPE)-**For managed WAN services saving equipment, transport and administrative cost

The Cisco 7200 VXR addresses these solution requirements by integrating functions previously performed by separate devices into a single platform. Through this integration, the Cisco 7200 VXR provides a single, cost-effective platform that supports:

• High-density LAN and WAN interfaces

• Broadband subscriber services aggregation, including PPP, RFC 1483 termination, and Layer 2 Tunneling Protocol (L2TP) tunneling

• Digital T1/E1 TDM trunk termination for voice, video, and data

• High-density multichannel T3/E3 and T1/E1 with integrated channel service unit/data service unit (CSU/DSU)

• ATM, Packet over SONET (POS), and Dynamic Packet Transport (DPT) connectivity

• ATM IMA (Inverse Multiplexing over ATM) for voice, video, and data

• Direct IBM mainframe channel connectivity

• Light-density Layer 2 Ethernet switching

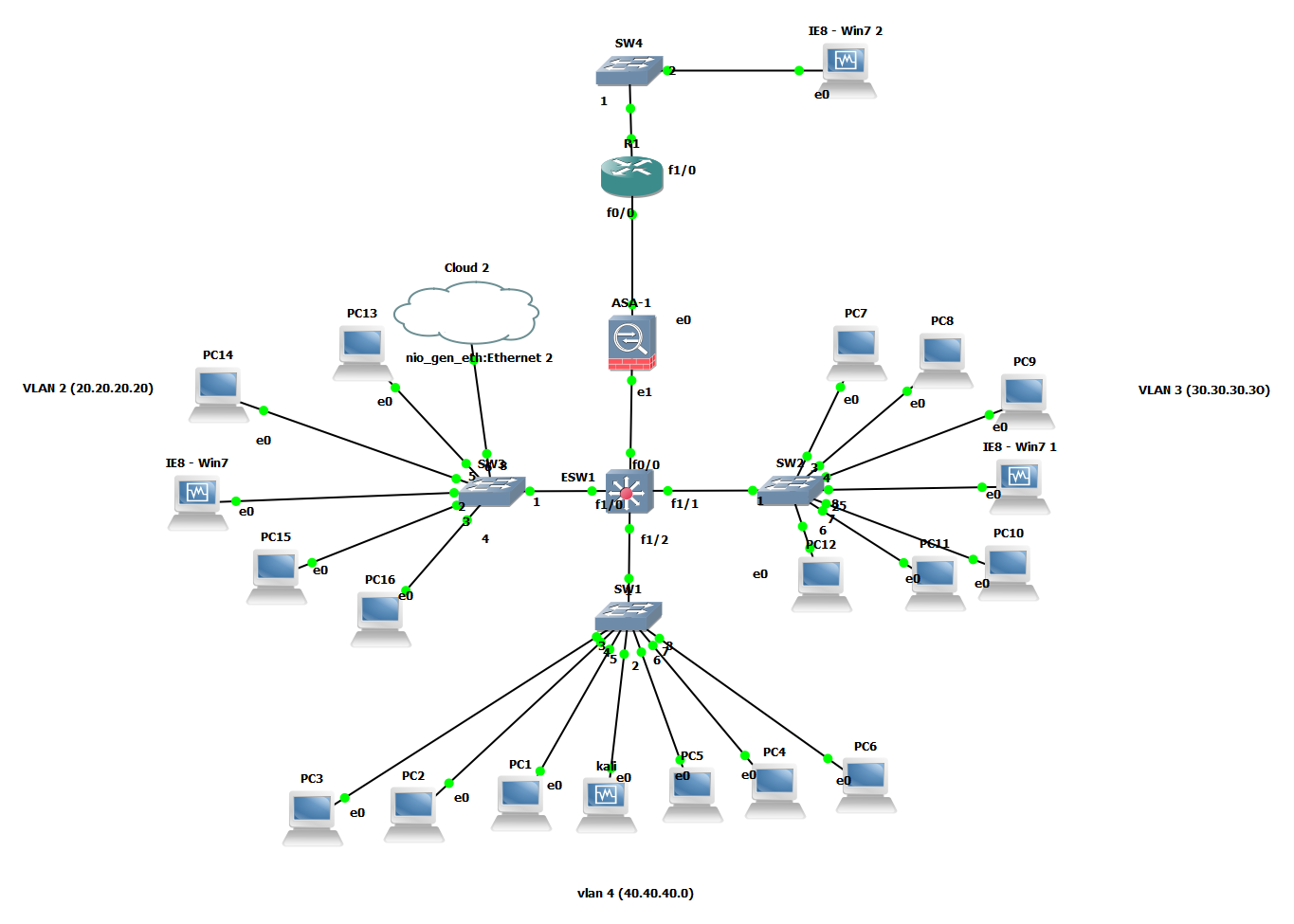
A **network switch** (also called **switching hub**, **bridging hub**, officially **MAC bridge**)is [networking hardwar](https://en.wikipedia.org/wiki/Networking_hardware)e that connects devices on a [computer networ](https://en.wikipedia.org/wiki/Computer_network)k by using [packet switchin](https://en.wikipedia.org/wiki/Packet_switching)g to receive, and forward data to the destination device.

A network switch is a multiport [network bridg](https://en.wikipedia.org/wiki/Network_bridge)e that uses [media access control addresse](https://en.wikipedia.org/wiki/Media_access_control_address)s to forward data at the [data link laye](https://en.wikipedia.org/wiki/Data_link_layer)r (layer 2) of the [OSI model](https://en.wikipedia.org/wiki/OSI_model). Some switches can also forward data at the [network layer](https://en.wikipedia.org/wiki/Network_layer)(layer 3) by additionally incorporating [routin](https://en.wikipedia.org/wiki/Routing)g functionality. Such switches are commonly known as layer-3 switches or [multilayer switches](https://en.wikipedia.org/wiki/Multilayer_switch).[[2]](https://en.wikipedia.org/wiki/Network_switch" \l "cite_note-layer3-2)

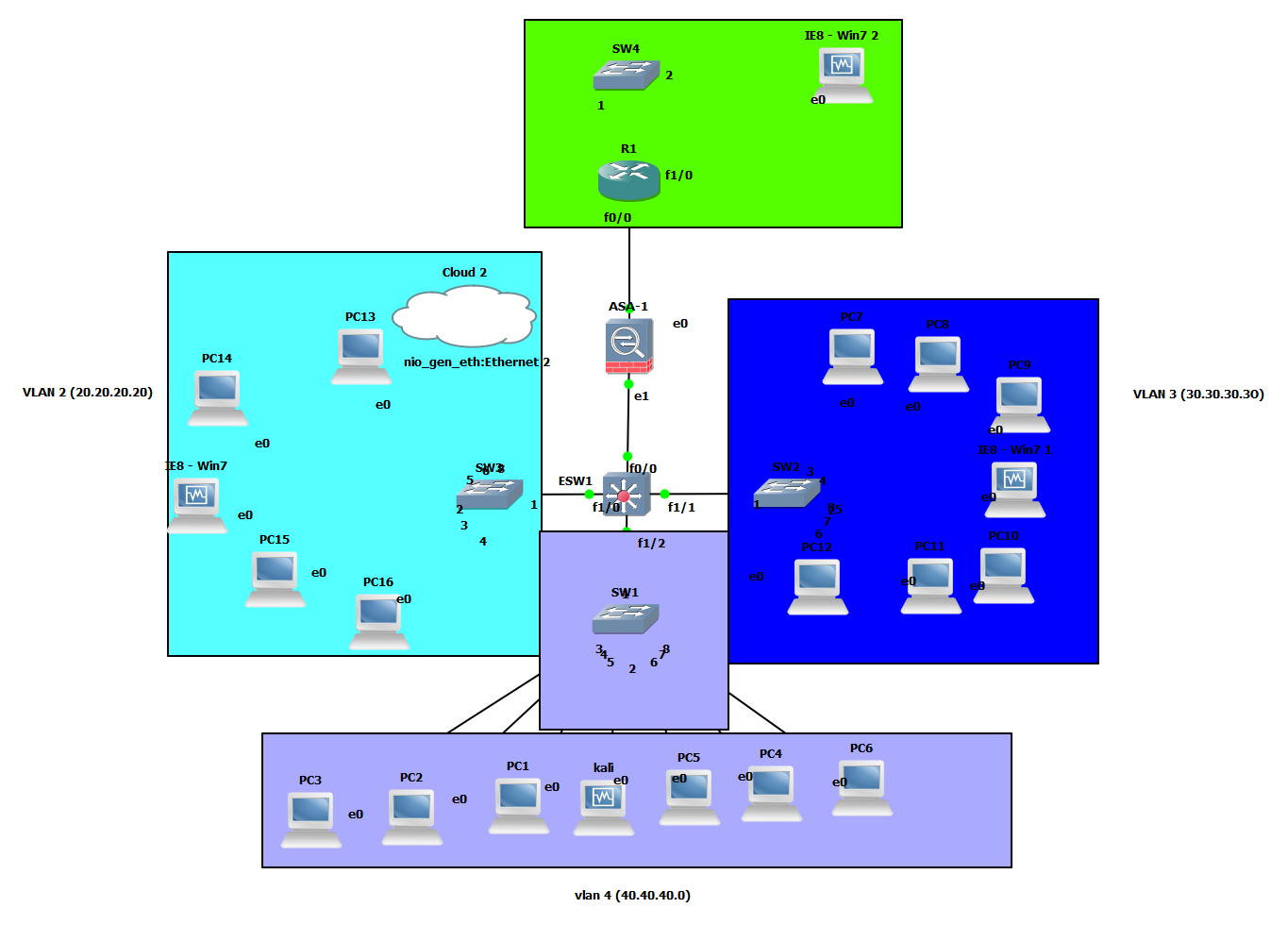
Switches for [Ethernet](https://en.wikipedia.org/wiki/Ethernet) are the most common form of network switch. The first Ethernet switch was introduced by [Kalpan](https://en.wikipedia.org/wiki/Kalpana_(company))a in 1990.Switches also exist for other types of networks including [Fibre Channel](https://en.wikipedia.org/wiki/Fibre_Channel), [Asynchronous Transfer Mode](https://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode), and [InfiniBand](https://en.wikipedia.org/wiki/InfiniBand).

Unlike less advanced [repeater hubs](https://en.wikipedia.org/wiki/Repeater_hub), which broadcast the same data out of each of its ports and let the devices decide what data they need, a network switch forwards data only to the devices that need to receive it.

Wireshark is a network or protocol analyzer (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyzer operates on Unix, Linux and Microsoft Windows operating system, and employs the GTK+ widget toolkit and pcap for packet capturing. Wireshark and other terminal-based free software versions like Tshark are released under the GNU General Public License dump. The difference is that it supports a graphical user interface (GUI) and has information filtering features.Wireshark permits us to see traffic passed through network.  
Features of Wireshark include:Data is analyzed either from the wire over the network connection or from data files that have already captured data packets.

* Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
* With the help of GUI or other versions, users can browse captured data networks.
* For programmatically editing and converting the captured files to the editcap application, users can use command line switches.
* Display filters are used to filter and organize the data display.
* New protocols can be scrutinized by creating plug-ins.
* Captured traffic can also trace Voice over Internet (VoIP) calls over the network.
* When using Linux, it is also possible to capture raw USB traffic.

**NETWORK LAYOUT**

****

**CONFIGURATION**

**ASA5505 CONFIGURATION**

hostname ciscoasa

enable password 8Ry2YjIyt7RRXU24 encrypted

passwd 2KFQnbNIdI.2KYOU encrypted

names

!

interface GigabitEthernet0

nameif OUTSIDE

security-level 0

ip address 209.165.201.1 255.255.255.0

!

interface GigabitEthernet1

nameif INSIDE

security-level 100

ip address 192.168.1.1 255.255.255.0

!

ftp mode passive

access-list 101 extended permit ip any any

access-list 101 extended permit icmp any any

pager lines 24

mtu OUTSIDE 1500

mtu INSIDE 1500

ip local pool VPNPOOL 1.1.1.2-1.1.1.100 mask 255.255.255.0

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

access-group 101 in interface OUTSIDE

!

router eigrp 1

network 0.0.0.0 0.0.0.0

!

http server enable

http 20.20.20.0 255.255.255.0 INSIDE

**CENTRAL LAYER 3 SWITCH**

interface FastEthernet0/0

description \*\*\* Unused for Layer2 EtherSwitch \*\*\*

ip address 192.168.1.2 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1

description \*\*\* Unused for Layer2 EtherSwitch \*\*\*

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet1/0

switchport access vlan 2

duplex full

speed 100

!

interface FastEthernet1/1

switchport access vlan 3

duplex full

speed 100

!

interface FastEthernet1/2

switchport access vlan 4

duplex full

speed 100

interface Vlan1

no ip address

shutdown

!

interface Vlan2

ip address 20.20.20.10 255.255.255.0

!

interface Vlan3

ip address 30.30.30.10 255.255.255.0

!

interface Vlan4

ip address 40.40.40.10 255.255.255.0

!

interface Vlan10

no ip address

!

interface vmi2

no ip address

!

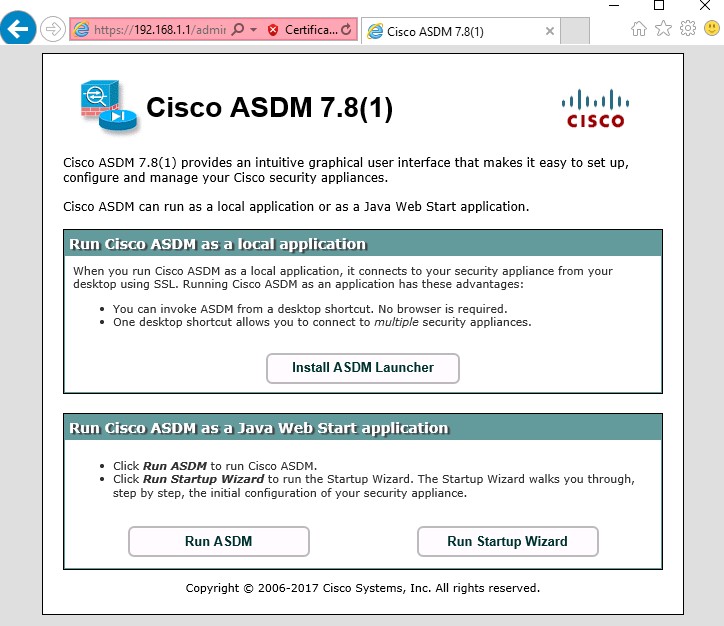
router eigrp 1

network 0.0.0.0

auto-summary

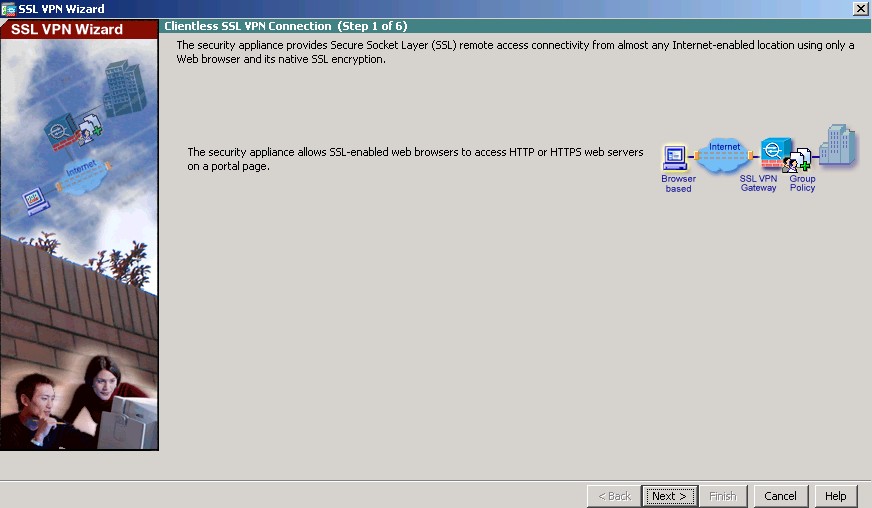
**CLIENTLESS VPN WITH ASDM**

Configuring Clientless SSL VPN Remote Access Using ASDM



### Step 1: Start the VPN wizard.

1. On the ASDM main menu, click Wizards>VPN Wizards>Clientless SSL VPN Wizard. TheClientless SSL VPN Connection screendisplays.



b.Review the on-screen text and topology diagram, and then click **Next** tocontinue.

### Step 2: Configure the SSL VPN user interface.

1. On the SSL VPN Interface screen, configure SSL-VPNas the Connection Profile Name, and specify outside as the interface to which outside users will connect.

Note: By default, the ASA uses a self-signed certificate to send to the client for authentication. Optionally, the ASA may be configured to use a third-party certificate that is purchased from a well-known certificate authority, such as VeriSign, to connect clients. In the event that a certificate is purchased, it may be selected in the Digital Certificate drop-down menu.

The SSL VPN Interface screen provides links in the Information section. These links identify the URLs that need to be used for the SSL VPN service access (log in) and for Cisco ASDM access (to access the Cisco ASDM software).

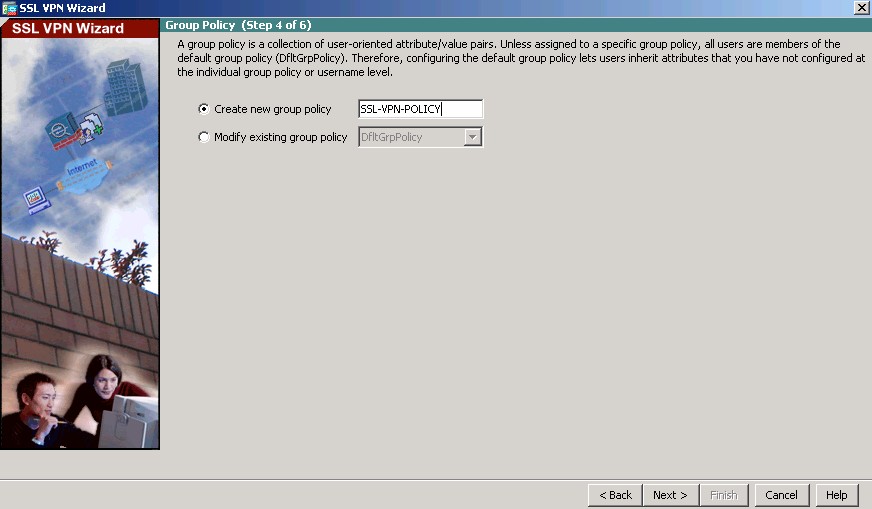
b. Click**Next**to continue.

### Step 3: Configure AAA user authentication.

1. On the User Authentication screen, clickAuthenticate using the local userdatabase.
2. Enter the user nameSSL-VPN-USERwith passwordcisco12345.
3. Click Add to create the new user and click Next tocontinue.

### Step 4: Configure the VPN group policy.

1. On the Group Policy screen, create a new group policy named SSL-VPN-POLICY. (When configuringa new policy, the policy name cannot contain anyspaces.)



1. Click **Next** to continue.

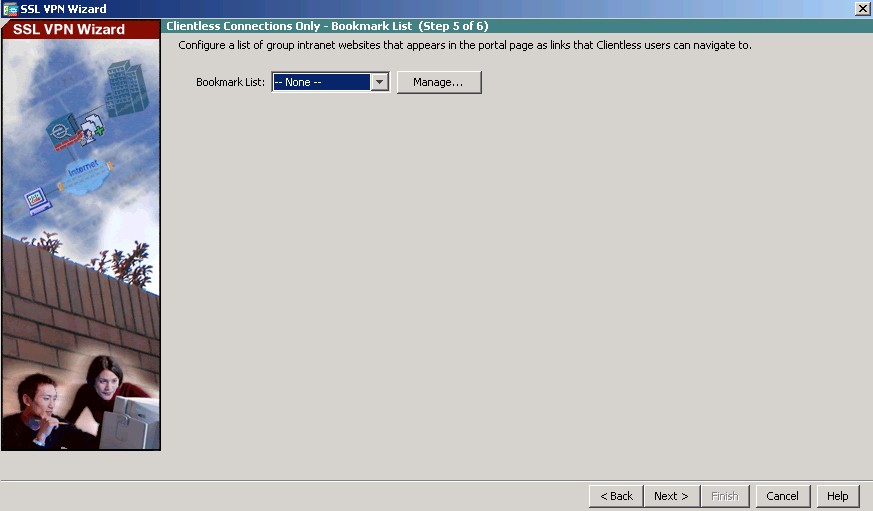
### Step 5: Configure the bookmark list (clientless connections only).

A bookmark list is a set of URLs configured to be used in the clientless SSL VPN web portal.

If there were bookmarks already listed, you would use the Bookmark List drop-down list, select the bookmark of choice, and click Next to continue with the SSL VPN wizard.

Note:There are no configured bookmark lists by default and, therefore, they must be configured by the network administrator.

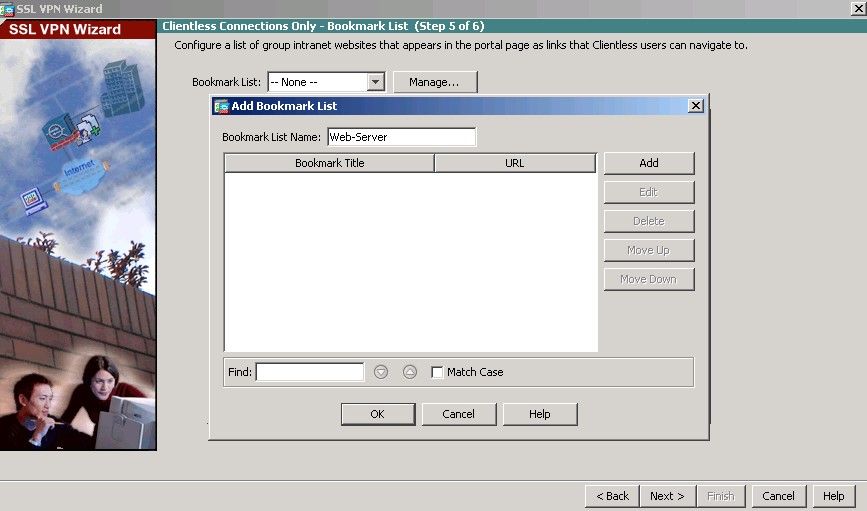
a. On the Clientless Connections Only – Bookmark List screen, click Manage to create an HTTP server bookmark in the bookmark list.

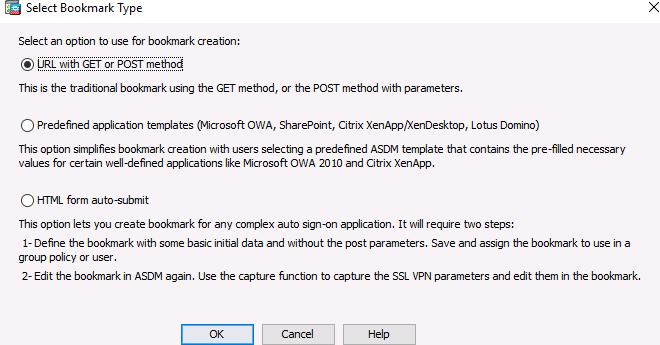


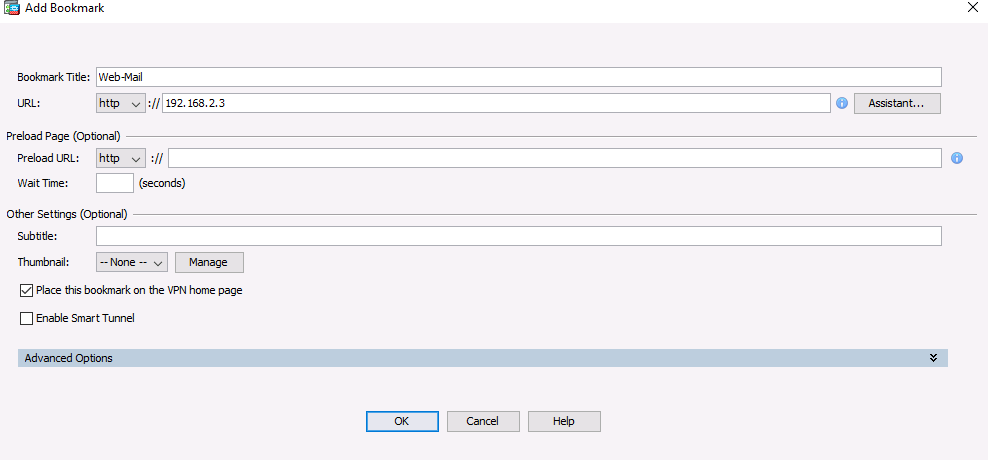
1. In the Configure GUI Customization Objects window, click Add to open the Add Bookmark List window. Name the list Web-Server.

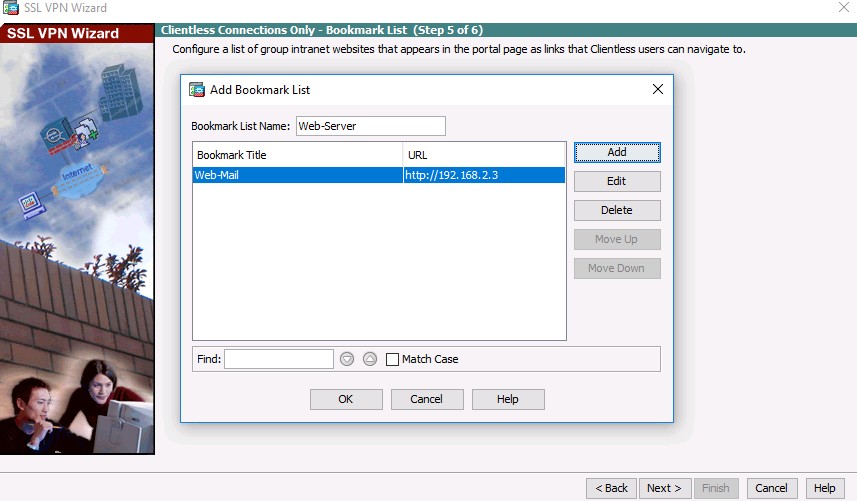
Note: If the Web-Server bookmark list is shown as available from a previous configuration, you can delete it in ASDM and re-create it.

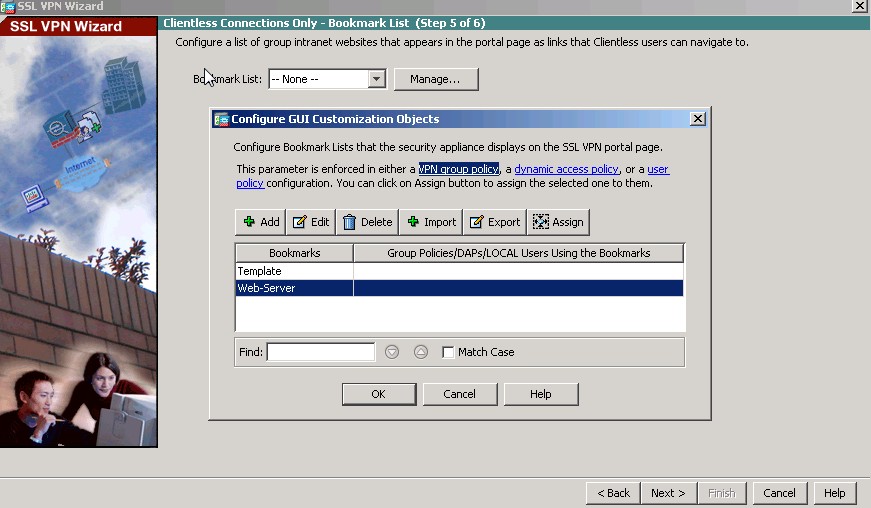
b.In the Add Bookmark List window, click Addto open the Select Bookmark Type window.

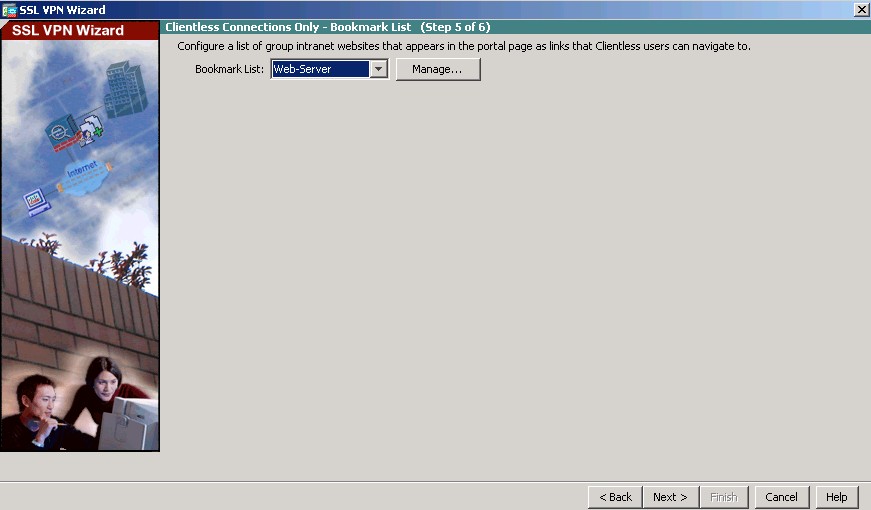


1. As shown in the figure, the ASDM can create three types of bookmarks. Select the URL with GET or POST method, clickOK.
2. Enter the bookmark title and enter the server destination IP address or hostname as the URL to be used with the bookmark entry. In this example, the Bookmark Title of Web-Mailis entered and an internal IP address of 192.168.2.3(the DMZ server) is specified.



1. Click OKto continue and return to the Add Bookmark List window which now displays the Web-Server bookmark title and URL.
2. Click OKto continue and return to the Configure GUI Customization Objects window which now show webs server bookmarks.

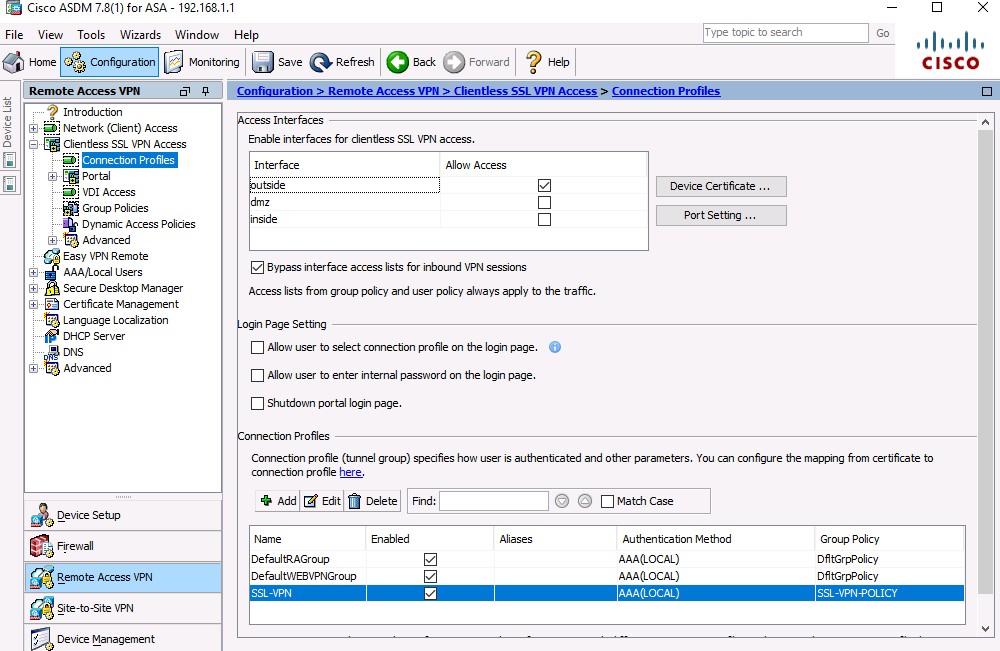


1. Click OK to continue and return to the Bookmark List window and click Next tocontinue.

### Step 6: Review the configuration summary and deliver the commands to the ASA.

The Summary page is displayed next. Verify that the information configured in the SSL VPN wizard is correct. Click Back to make changes, or click Cancel and restart the VPN wizard. Click Finish to complete the process and deliver the commands to the ASA

### Step 7: Verify the ASDM SSL VPN connection profile.

In ASDM, click Configuration>Remote Access VPN>Clientless SSL VPN Access>Connection Profiles. In this window, the VPN configuration can be verified and edited.

### Step 8: Verify VPN access from the remote host.

1. Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (https://209.165.200.226). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA.

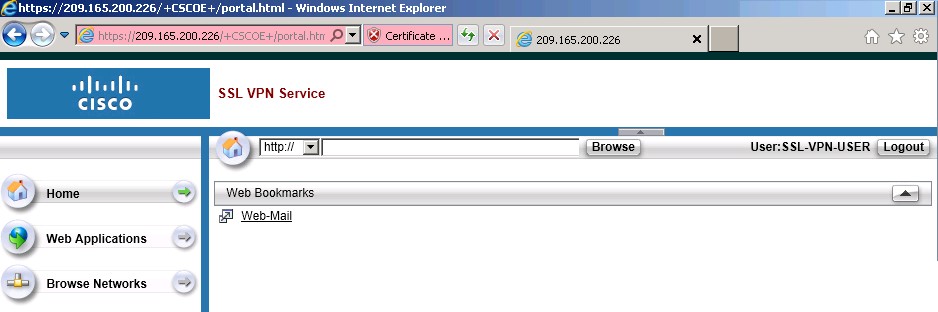
Note: If you encounter a prompt stating that the connection is not trusted or secure, accept the self- signed certificate to continue.

1. The Logon window should display. Enter the previously configured username SSL-VPN-USER and password and click Logon to continue.

### Step 9: Access the web portal window.

After the user authenticates, the ASA SSL web portal page lists the various bookmarks previously assigned to the profile. If the Bookmark points to a valid server IP address or hostname that has HTTP web services installed and functional, the outside user will be able to access the server from the ASA portal.

**Note:**In this lab, the web mail server is not installed.



**FUTURE SCOPE OF THE PROJECT**

*This project is used to implement basic security measures in an small level organization. As we using web based vpn so its easy for any client use its web to access ant data by providing the appropriate credentials and vpn will provide layer 3 security . As internet is used to special connnection is needed , so reduce cost to access data remotely and encryption by ssl vpn will take care for data security over internet.*

**References**

[1]https://networklessons.com/cisco/asa-firewall.

[2]https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa\_90\_cli\_config/interface\_start\_5505.html.

*[3]https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.*