Agenda

- Introduction to Cisco IOS® SSL VPN
- Positioning and Use Cases
- Technology Overview
  - Advanced Full-Network Access
  - Comprehensive Endpoint Protection
  - Ease of Deployment and Management
  - SSL VPN Gateway Network Integration
SSL VPN-Based Remote Access

Solution Characteristics

What is SSL VPN?

- Allows remote access using a Web browser and SSL encryption
- Does not require preinstalled client software
- Enables access from company-managed and non-company managed user desktops

Why does SSL VPN appeal to customers?

- No preinstalled desktop software = Lower administration and operations costs
- Access from any desktop solves the complexity of secure contractor and business-partner access
- Easy to use from the end users’ perspective
- Offers Web portals that can be customized on a per-user basis
Secure Sockets Layer Overview

- SSL VPN uses the SSL protocol to enable secure transactions of data through privacy, authentication, and data integrity.
- Capability shipped by default in leading browsers.
  Protocol developed by Netscape for secure e-commerce.
- Relies on certificates, public keys, and private keys.
- Creates secure session between browser and server.
  Authenticated (RSA) and encrypted (RC4, 3DES, and DES).
- `https://` Usually over port 443.
  Closed lock indicates SSL enabled.
SSL VPN Is Different from E-Commerce

- More advanced than SSL offloading of Web pages
- Must fit into existing networks and application environments
- Must support all the same authentication mechanisms and often extensive application list as IPsec
How Cisco IOS® SSL VPN Works

- Advanced full-network tunneling client pushed down to remote client PC
- End user works in a “sandbox”: a virtual desktop that provides comprehensive session protection and erases leftover data
- Wizard-driven interface makes it easy to set up and manage the SSL VPN gateway
- Contexts and VPN routing and forwarding (VRF) integration allow virtualization
Cisco IOS® SSL VPN
Positioning and Use Cases
Cisco IOS® SSL VPN Positioning
For Enterprise Branch Offices and Small and Medium-Sized Businesses (SMBs)

**SMBs: Integrated Solution**
- SSL VPN adds significant value to security router investment.
- Cisco® IOS Software security routers offer the only one-box solution for IPsec, SSL VPN, firewall, intrusion prevention system (IPS), routing, etc.
- Cisco IOS SSL VPN offers an affordable, easy-to-use solution.

**Enterprise: Distributed Branch-Office Access**
- Branch-office router-based SSL VPN provides efficient remote access to local (branch) resources.
  - Faster response time versus access to central gateway and back through the WAN
- Access policies are in line with users’ configurations at work.
  - Redirection from central gateway requires setting up additional access control lists (ACLs) and tunnels
- The branch SSL VPN gateway backs up the central gateway for redundancy and disaster recovery.
Enterprise Branch Teleworker Design
Example: Regional Law Firm with Multiple Offices

SSL VPN Remote Access
- No software to install and maintain on PCs
- Full tunnel provides secure access to Citrix and e-mail applications
- Endpoint security with Cisco Secure Desktop

VPN Aggregation for IPsec and SSL
- Provides efficient remote access to local resources
- Provides access policies that are in line with users' configurations at work
- Backs up central gateway for redundancy and disaster recovery

Table:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-road access to business applications</td>
<td>Improved staff productivity</td>
</tr>
<tr>
<td>Remote access to corporate network as well as local resources</td>
<td>Faster response time; offload concentrator main office</td>
</tr>
<tr>
<td>Integrated application firewall, inline intrusion prevention, and touchless endpoint security</td>
<td>Proactive threat defense</td>
</tr>
</tbody>
</table>
**SMB Design**

**Single Box Solution for Remote Access and Voice**

- **SSL VPN remote access**
  - Full tunnel to provide secured data and voice communication
  - Multiple OS support: Microsoft Windows (XP and Vista), Mac OS X, and Linux
  - Endpoint security with Cisco Secure Desktop

- **Integrated VPN, security, routing, and interprocess communication (IPC) services**
  - Single box to operate and manage.
  - Provides SSL VPN remote access as well as traditional IPsec client features including split tunneling and network extension
  - Integrated certificate authority server
  - Built-in or external authentication, authorization, and accounting (AAA) user authentication

---

<table>
<thead>
<tr>
<th>Capability</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides SSL VPN and voice service in existing router</td>
<td>Adds significant value to security router investment</td>
</tr>
<tr>
<td>One phone number to call; voice security is transparent to end user</td>
<td>Simplified user experience</td>
</tr>
<tr>
<td>Significant phone bill reduction</td>
<td>Reduced total cost of ownership (TCO)</td>
</tr>
</tbody>
</table>
Service Provider Design

MPLS Integration with VRF

- Service providers can put specific Internet routes into a VRF and transparently integrate the SSL VPN gateway into a shared MPLS network
- Increased security by separating specific routes from global routing table
- Support for overlapping IP address pools
Technology Overview
Cisco IOS® SSL VPN Highlights

- **Advanced full-network access**
  
  Cisco® AnyConnect VPN Client provides full-tunnel access for virtually any application, such as Cisco IP SoftPhone; dynamically loaded client can be permanently installed or uninstalled after disconnect

- **Comprehensive endpoint protection**
  
  Cisco Secure Desktop prevents digital leakage and protects user privacy; easy to implement and manage; works with desktop guest permissions

- **Ease of deployment and management**
  
  Simple GUI-based provisioning and management with step-by-step wizards for easy deployment

- **SSL VPN gateway network integration**
  
  Advanced authentication and access control with embedded certificate-authority server; virtualization allows segmentation as well as pooling of resources while masking the physical attributes and boundaries of the resources
Cisco IOS® SSL VPN Solution Overview

- Advanced Full-Network Access
- Comprehensive Endpoint Security
- Ease of Deployment and Management
- Network Integration
Advanced Full-Network Access
Cisco® AnyConnect VPN Client

- Extends the in-office experience
  LAN-like full-network access; supports latency-sensitive applications such as voice

- Access across platforms
  Windows 2000, XP (x86 and x64), and Vista (x86 and x64)
  Mac OS X and Linux Intel

- Always up-to-date
  Remotely installable and configurable to minimize user demands

- No-hassle connections
  No reboots required
  Standalone, start work before login, Web launch, and portal connection
  MSI: Windows pre-installation package
Advanced Full-Network Access
VPN Client Features and Benefits

Uses depth of Cisco® encryption client experience to deliver an advanced, stable, and easy-to-support SSL VPN tunneling client: Cisco AnyConnect VPN Client

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec-like application access through Web-pushed client</td>
<td>Application-agnostic full-network access</td>
</tr>
<tr>
<td>Touchless central-site configuration</td>
<td>Low operating cost</td>
</tr>
<tr>
<td>Compatible with Cisco IP SoftPhone for voice-over-IP (VoIP) support</td>
<td>Multimedia data and voice desktops for greatest user productivity</td>
</tr>
<tr>
<td>Client may be either removed at end of session or left permanently installed</td>
<td>No trace of client after session; provides better security</td>
</tr>
<tr>
<td>No reboot required after installation</td>
<td>Improved productivity and better user satisfaction</td>
</tr>
</tbody>
</table>
Advanced Full-Network Access

VPN Client Activation: Web Launch

- Start Full Tunnel Client Connection

functions svc-required | enabled
- svc-required: Bypasses the portal page
- enabled: Start button shows up on the portal page
Advanced Full-Network Access
VPN Client: Standalone Connect

- Type or select a remote peer from the pull-down list to connect to https://sslvpn-demo.cisco.com/tunnel

- Prompts for user credentials
Advanced Full-Network Access
Minimal End-User Support Burden

- Full network experience
- Silent, reliable, behind-the-scenes operation

Cisco AnyConnect VPN Client

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:
Advanced Full-Network Access

SSL VPN Full Tunnel Establishment

---

**TCP Connect (Port x or Default 443)**

1. **Initiate SSL Handshake**
2. **SSL Server Certificate (Chain)**
3. **Completed Handshake**
4. **Username and Password**
5. **Push Down SSL VPN Client**

---

- After SSL handshake is initiated, client continues to:
  - Obtain server certificate chain from system Library
  - Authenticate gateway certificate (chain) and check revocation (except root certificate authority)

- If revoked or severe error: Tear down connection

- If moderate error: Ask user to view certificate and accept or deny; if user denies certificate chain, tear down connection
Advanced Full-Network Access
Gateway Configuration

```
ip local pool mypool 192.168.1.2 192.168.1.100  # Address pool must be part of a subnet already defined on the router interface
!
webvpn gateway ssl-vpn
  ip address 1.1.1.8 port 443
  ssl trustpoint golden-tp
  inservice
!
webvpn context contextA
  ssl trustpoint
  ssl authenticate verify all
  inservice
!
policy group mypolicy
  functions svc-required  # enabled: Use Start button on portal page
  svc address-pool "mypool"  # Apply address pool configured above
  svc keep-client-installed
  svc split include 192.168.0.0 255.255.0.0  # Traffic to this subnet will be encrypted
default-group-policy mypolicy
gateway ssl-vpn domain domainA
inservice```
Advanced Full-Network Access

Downloading the VPN Client

- Cisco® AnyConnect VPN Client software package files can be downloaded from:
  
  http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

- Package files can be installed using Cisco Security Device Manager (SDM) 2.5 or later
  
  Cisco AnyConnect VPN Client is supported on Cisco IOS® 12.4(15)T and later

- Alternatively, download the client to the router flash memory and install using the following command:

  ```
  webvpn install svc flash:/webvpn/<package_name>
  sequence <num>
  ```
Advanced Full-Network Access
Troubleshooting the VPN Client

For Cisco® AnyConnect VPN Client installation issues, obtain the following files:

- **VPN downloader log file:**
  \Windows\setupapi*.log

- **MSI installer log file:**
  \Documents and Settings\<username>\Local Settings\Temp\anyconnect-win-2.0.xxxx-k9-install-yyyyyy.log

  Obtain the most recent file for the version of the client you are trying to install.

- **PC system information (process may take a few minutes to complete):**
  XP/2K: winmsd /nfo c:\system_info.nfo
  Vista: msinfo32 /nfo c:\system_info.nfo
Advanced Full-Network Access
Troubleshooting the VPN Client

For Cisco® AnyConnect VPN Client connection issues:

- On the client PC, obtain the AnyConnect log from the Windows Event Viewer.
- Windows:
  Choose Start > Run and enter eventvwr.msc /s.
  Right-click Cisco® AnyConnect VPN Client log and select Save Log File As. Be sure to save the file in .evt format (evtx for Vista).
- Non-Windows:
  /var/log/system.log, etc.
## Advanced Full-Network Access

### Cisco® VPN Clients Comparison

<table>
<thead>
<tr>
<th>Function</th>
<th>Cisco VPN Client (IPsec Client)</th>
<th>Older Cisco SSL VPN Client</th>
<th>Cisco AnyConnect VPN Client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approximate size</strong></td>
<td>10 MB</td>
<td>400 KB</td>
<td>3 MB</td>
</tr>
<tr>
<td><strong>Initial installation</strong></td>
<td>Distribute</td>
<td>Auto download Distribute</td>
<td>Auto download Distribute</td>
</tr>
<tr>
<td><strong>Administrator rights requirement for installation</strong></td>
<td>Required</td>
<td>For initial installation only (stub installer available)</td>
<td>For initial installation only (MSI available on Windows)</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>IPsec</td>
<td>TLS (HTTPS)</td>
<td>DTLS***, TLS (HTTPS) (Auto)</td>
</tr>
<tr>
<td><strong>OS support</strong></td>
<td>Multiple*</td>
<td>Windows 2000 and XP</td>
<td>Multiple**</td>
</tr>
<tr>
<td><strong>Head-end</strong></td>
<td>Cisco ASA and IOS Software</td>
<td>Cisco ASA and IOS Software</td>
<td>Cisco ASA and IOS Software</td>
</tr>
</tbody>
</table>

* Windows 2000, XP, x86, and Vista x86; Mac OS X 10.4; Linux Intel 2.6; and Solaris

** Windows 2000, XP x86 and x64, and Vista x86 and x64; Mac OS X 10.4 and 10.5; Linux Intel 2.6; and Windows Mobile 5 and 6 support planned (additive license); non-Windows support and alternate connection modes available, including Datagram Transport Layer Security (DTLS) for Cisco ASA 8.0+ only

*** DTLS is not supported with the Cisco IOS head-end.
Cisco IOS® SSL VPN Solution Overview

- Advanced Full-Network Access
- Comprehensive Endpoint Security
- Ease of Deployment and Management
- Network Integration
Comprehensive Endpoint Security
SSL VPN Endpoint Security Challenges

Before SSL VPN Session
Who owns the endpoint?
Endpoint security posture: Antivirus program and personal firewall?
Is malware running?

During SSL VPN Session
- Is session data protected?
- Are typed passwords protected?
- Has malware launched?

Post-SSL VPN Session
- Browser cached intranet Webpages?
- Browser stored passwords?
- Downloaded files left behind?
Comprehensive Endpoint Security
How Cisco® Secure Desktop Works

Complete Preconnect Assessment
- Location assessment: Managed or unmanaged desktop?
- Security posture assessment: Antivirus program operational and up-to-date, personal firewall operational, malware present?

Comprehensive Session Protection
- Data sandbox and encryption that protects every aspect of session
- Malware detection with hooks to Microsoft free antispyware software

Postsession Clean-Up
- Encrypted partition overwrite (not just deletion) using Department of Defense (DoD) algorithm
- Cache, history, and cookie overwrite
- File download and e-mail attachment overwrite
- Autocomplete password overwrite
Comprehensive Endpoint Security
Inside Cisco® Secure Desktop

Works with Desktop
Guest Permissions
No Administrator Privileges Required
Comprehensive Endpoint Security
Cisco® Secure Desktop Package File

- Cisco Secure Desktop package file
  
  The Cisco Secure Desktop software package can be downloaded from: http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

  Package file already bundled with Cisco Security Router bundles; transparent installation since Cisco Security Device Manager (SDM) 2.3

- Cisco IOS® SSL VPN supports Cisco Secure Desktop package file up to Version 3.1

- Install Cisco Secure Desktop on router using the following command:
  
  ```bash
  webvpn install csd flash:/webvpn/csd3x.pkg
  ```
Comprehensive Endpoint Security
Cisco® Secure Desktop Configuration

gateway gw-1
  ip address 192.168.22.103 port 443
  ssl trustpoint SSLVPN
  inservice
webvpn context contextA
  csd enabled
webvpn install csd flash:/webvpn/sdesktop.pkg
Comprehensive Endpoint Security
Cisco® Secure Desktop Administration

- Log in to https://<gateway>/csd_admin.html
Create at least one location for each context: for example, home or office.

Define criteria to match for this location.

Enable keystroke logger detection.

Define endpoint assessment policies.
Cisco IOS® SSL VPN Solution Overview

- Advanced Full-Network Access
- Comprehensive Endpoint Security
- Ease of Deployment and Management
- Network Integration
Ease of Deployment and Management

Cisco® Router and Security Device Manager

- Fast and easy deployment and management of integrated services on Cisco IOS® routers
- Easy-to-use, Web-based GUI for single device management for site-to-site VPN, remote access VPN, IPS, firewall, etc.
- Less than 30 minutes to deploy fixed-configuration Cisco Integrated Services Routers
- Featured on Cisco 800 Series and 7301 Routers; loaded from factory at no additional cost
- Supported in seven international languages

“Cisco Router and Security Device Manager significantly reduces technical expertise required to configure Cisco routers.”

ED MIER, MIERCOM
Ease of Deployment and Management
Integrated SSL and IPsec Management

- Separate wizards to configure SSL VPN, Easy VPN, and Dynamic Multipoint VPN (DMVPN)
Ease of Deployment and Management
SSL VPN Wizard: Basic Setup

- Define context name
- Set up portal IP address
- Define the domain name for this context
- Login URL includes domain name
- SSL authentication through digital certificates

SSL VPN Wizard

IP Address and Name
This is the IP address users will enter to access the SSL VPN portal page. If multiple SSL VPN services are configured in this router, the unique name is used to distinguish the service.

IP Address: 172.19.111.136
Name: contextA

Domain: domainA

Digital Certificate
When users connect, this digital certificate will be sent to their web browser to authenticate the router.

Certificate: TP-self-signed-539420202

URL to login to the SSL VPN service: https://172.19.111.136domainA
Ease of Deployment and Management
SSL VPN Wizard: User Authentication

- User authentication can be local or external using RADUS, Cisco Access Control Server, etc.
Ease of Deployment and Management
SSL VPN Wizard: Pools and Other Options

- Set up IP address pools (must be part of directly connected subnets or in the same subnet as a loopback interface)
- Specify Cisco® AnyConnect VPN client location
- Retain the client software on user PCs to reduce demands on bandwidth

- Includes split tunneling and split Domain Name System (DNS)
Ease of Deployment and Management
SSL VPN Wizard: Includes and Excludes

- Specify Include Traffic—traffic that needs to be encrypted and go through the tunnel.
- Specify Exclude Traffic—traffic that will be in clear-text: for example, bound for Internet destinations.
Ease of Deployment and Management

SSL VPN Wizard: Themes

- Custom portals—Use themes to define colors, text, and logos.
Cisco IOS® SSL VPN Solution Overview

- Advanced Full-Network Access
- Comprehensive Endpoint Security
- Ease of Deployment and Management
- Network Integration
SSL VPN Gateway Network Integration

Contexts

- Contexts are logical groups that can be used to segregate extranet partners or internal enterprise departments within a single SSL VPN gateway.
- When the user logs in, a determination is made to which context the user belongs.
- Resources associated with the context will then be used for that user.
SSL VPN Gateway Network Integration

Contexts and Policy Groups

- Each SSL VPN gateway supports multiple contexts.
- Each context supports multiple policy groups.

Policy groups are local to the context; not shared across contexts

WebVPN Gateway

WebVPN Context c1
- AAA Authorization List
- AAA Authorization Domain
- Enable or Disable Cisco Secure Desktop
- Default Policy Group
- Associated Gateway
- Enable or Disable
- Login Message
- Title
- ...

WebVPN Context c2
- AAA Authorization List
- AAA Authorization Domain
- Enable or Disable Cisco Secure Desktop
- Default Policy Group
- Associated Gateway
- Enable or Disable
- Login Message
- Title
- ...

Policy Group
- SVC
- ...

Policy Group
- SVC
- ...
SSL VPN Gateway Network Integration

One-Gateway-to-One-Context Model

- Multiple contexts and multiple gateway configurations can coexist.
- In the one-gateway-to-one-context model, each context belongs to a separate gateway; the gateway IP address in the packet identifies the associated context.

```
webvpn gateway SALES-DEP
    ip address 208.42.0.12 port 443
    ssl trustpoint tp1
    inservice
!
webvpn gateway MKT-DEP
    ip address 209.42.0.12 port 443
    ssl trustpoint tp1
    inservice
!
webvpn context sales-cxt
    gateway SALES-DEP
!
webvpn context marketing-cxt
    gateway MKT-DEP

https://208.42.0.12/  ← Use IP address to differentiate gateway
https://209.42.0.12/
```
SSL VPN Gateway Network Integration
One-Gateway-to-Many-Contexts Model

- In the one-gateway-to-many-context model, the same gateway is used for multiple contexts (more common usage).

```plaintext
webvpn gateway common-gateway
    ip address 208.42.0.12 port 443
    ssl trustpoint tp1
    inservice
!
webvpn context SALES-DEP
    gateway common-gateway domain sales
!
webvpn context MKT-DEP
    gateway common-gateway domain marketing

https://208.42.0.12/sales/ ➔ Use domain to differentiate context
https://208.42.0.12/marketing/
```
### SSL VPN Gateway Network Integration

**MPLS Integration with VRF**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign specific routes to VRF</td>
<td>Transparently integrates with MPLS-based network</td>
</tr>
<tr>
<td>Separate specific routes from the global routing table</td>
<td>Increased security; overlapping IP address pools support</td>
</tr>
</tbody>
</table>

**Virtualization to Integrate with Multiprotocol Label Switching (MPLS) Network**

- **Remote Access**
  - Telecommuter
  - Mobile Worker
  - Dialup and Wireless

- **Public Internet**
  - DSL and Cable
  - POP

- **Service Provider Shared Network**
  - SSL-VPN-SG
  - PE

- **Corporate Intranet**
  - Customer A
  - Customer B
  - Customer C

**Network Elements**

- **Internet VRF**
- **Global VRF**
- **VPN A**
- **VPN B**
- **VPN C**
SSL VPN Gateway Network Integration
VRF Configuration

```plaintext
ip vrf fvrf_1
   rd 100:3
!
ip vrf vrf_A
   rd 100:1
!
interface FastEthernet1/1.12
   encapsulation dot1Q 12
   ip vrf forwarding fvrf_1
   ip address 192.168.122.103 255.255.255.0
!
interface FastEthernet1/1.13
   encapsulation dot1Q 13
   ip vrf forwarding vrf_A
   ip address 10.1.1.22 255.255.255.0
!
```

```plaintext
webvpn gateway gw_A
   vrf-name fvrf_1
   ip address 208.20.0.71 port 443
   ssl trustpoint tp1
   inservice
webvpn context cxt_A
   vrf-name vrf_A
   gateway gw_A domain domain1
```
SSL VPN Gateway Network Integration

Authentication and Access Control

- Robust authentication
  - Digital certificates for SSL authentication
  - RADIUS or AAA to manage users

- Advanced network access control options
  - IP address, differentiated services code point and type of service (DSCP/ToS), TCP/User Datagram Protocol (UDP) port, per user, and per group
SSL VPN Gateway Network Integration

AAA Authentication

1. User initiates SSL VPN session
   • https://172.19.217.93/sales
   • Enters the login page:
     username: ssluser1
     password: ********

2. User mapped to context VPN1
   • The WebVPN context forwards the login information to AAA

3. AAA authenticates user
   • Sends back any attribute AV-pairs to the context for that user session

4. Authenticated user in session
   • After authentication, a user session is set up with policy group and other context information
   • Attributes pushed down from the AAA server override configured values

5. Access internal server
SSL VPN Gateway Network Integration

AAA Authentication: Configuration

- AAA method list associated with context is used to authenticate the user: Different contexts can have different AAA method lists.

- Accounting: Create global accounting configuration and within the desired context; Cisco IOS® Software supports start, stop, and update accounting records.

```
aaa authentication login webvpn group radius
aaa authentication login webvpn1 local
aaa accounting network default start-stop group radius
!
webvpn context c1
  aaa authentication list webvpn
  aaa accounting list default
!
webvpn context c2
  aaa authentication list webvpn1
```
SSL VPN Gateway Network Integration
Embedded Certificate Authority

- Offers standalone certificate-authority server embedded into Cisco IOS® Software
- Allows easy certificate deployment
- Includes certificate revocation services
- Enrollment through browser after administrator grants permission
SSL VPN Gateway Network Integration

Trustpoint and Certificate Authority Setup

- Each SSL VPN gateway requires a trustpoint to be configured.
  
  One trustpoint per WebVPN gateway is recommended.

- The trustpoint contains the certificate authority that signed the certificate in use by SSL VPN; the SSL key is generated per session during the handshakes.

  The trustpoint can be shared among multiple gateways.

- The certificate can be generated using Cisco IOS® certificate authority server or downloaded from external certificate authority servers.

  The SSL VPN gateway can configured with a valid x509v3, issued by a trusted certificate authority (VeriSign, Entrust, Thawte, etc.) or a private certificate authority (OpenSSL, Microsoft Certificate Authority, etc.).
SSL VPN Gateway Network Integration
Generating Certificates

Utilizing Cisco® Certificate Authority Server

- A persistent self-signed certificate is the easiest way to configure a trustpoint and associate it with the gateway.

- You can generate a persistent self-signed certificate using the following configurations:

  ```
  Router(config)# crypto pki trustpoint local
  Router(ca-trustpoint)# enrollment selfsigned
  Router(config)# crypto pki enroll local
  ```
aaa new-model
aaa authentication login LOCAL local
!
hostname ios_router
ip domain name cisco.com
ip name-server 1.1.1.1
!
crypto pki trustpoint TP-self-signed-1653287141
    enrollment selfsigned
    revocation-check none
    rsakeypair TP-self-signed-1653287141
!
interface FastEthernet0
    ip address 192.168.10.100 255.255.255.0
    description Internet facing interface
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1

Cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html
Summary: Cisco IOS® SSL VPN Advantages

- Advanced full-network client access
- Comprehensive endpoint security
- Easy to set up and manage
- Gateway network integration for authentication and virtualization
- Low cost of ownership
  - One device for IPsec, SSL, firewall, IPS, and routing
  - Simple, cost-effective licensing
  - Integrated management for VPN, security, and routing functions (Cisco SDM and Cisco Security Manager)
Additional Information

- Cisco.com Webpage
  
  www.cisco.com/go/ioswebvpn

- E-mail
  
  ask-stg-ios-pm@cisco.com

- Acknowledgments
  
  This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).