Cisco Virtual Office: Layered Security Features

This guide provides detailed design and implementation information relating to the different layered security features in the Cisco® Virtual Office.

Please refer to the Cisco Virtual Office overview (http://www.cisco.com/go/cvo) for more information about the solution, its architecture, and all of its components.

Purpose and Scope

This guide explains how the layered security approach is implemented in the Cisco Virtual Office solution. This deployment can be used as a baseline for similar remote-access, site-to-site VPN, and managed service provider VPN deployments. This document does not explain all the alternative designs or different configurations, nor does it explain the zone-based security features. Please refer to the Advanced Layered Security Features guide for the zone-based security features (Reference 21).

Introduction

Following are the major features included in this guide:

User and Device Security and Authentication

- Authentication Proxy (AuthProxy)
- IEEE 802.1x-based user authentication
- Secure Address Resolution Protocol (ARP)

Router Security and Authentication

- RSA keys and certificates
- Public key infrastructure (PKI) with authentication, authorization, and accounting (AAA)
- RSA key erase on password recovery
- RSA key locking
- Disabling password recovery
- Restricting console access
- Disabling console access

Network Security

- Stateful Firewall—Legacy
- Intrusion prevention system (IPS)

Domain Separation

- Split Domain Name System (DNS)

Hardware and Software

This guide is based on a Cisco 881 Integrated Services Router with wireless running Cisco IOS® Software Release 12.4(20)T. The FastEthernet4 interface connects to the Internet service provider (ISP). Two internal networks are configured using VLANs, namely VLAN10 and VLAN20. They are called ”trusted” network and “guest” network in this guide. The devices such as IP phone, computer, etc. that need corporate access are connected to the trusted network. Other devices that do not need corporate access are connected to the guest network. The guest network is optional. For other Cisco router platforms, the sample configurations may need minor modifications.

User and Device Security and Authentication

The security and authentication features mainly ensure that only authorized users and devices can access the corporate network.

Authentication Proxy

A remote-office network may not be physically as secure as the corporate environment, meaning that nonemployees also may have access to the devices connected to the spoke router. Authentication Proxy provides a way to identify legitimate users and limit access to the corporate network to only those users. Auth-proxy can be used to provide role based access permissions to the users.

All access to the corporate network is denied by an inbound access control list (ACL) applied on the inside interface of the router. To initiate the authentication process user will have to first access a corporate website using a Web browser. This access will be intercepted by the router and will be replaced with a web based user authentication prompt. The user will be allowed to have access to the corporate site only if correct credentials are provided. The credentials are verified by a RADIUS server. Upon verification of the credentials, appropriate permit access control entries (ACEs) are downloaded and applied on the spoke router, based on the credentials. It is possible to download a “permit ip any any” for all users or to download specific ACEs based on the group to which the user belongs. This way the network administrator can implement role-based access control.

The authentication process begins when a user initiates web access using HTTP. FTP and Telnet can also be configured to initiate the authentication. The traffic that initiates authentication process is defined by an intercept ACL.

The authenticated sessions can be configured to time out after an absolute timeout or inactivity timeout, whose values are configurable. An inactivity timer triggers if there is no traffic from the client computer for the configured period of time. If any of the timers is triggered, the authentication cache is cleared, and you have to reauthenticate.

If a computer is disconnected from the network, the authentication cache remains until the inactivity timeout occurs. Before the cache is expired, a different computer can use the same IP address and continue to use the authenticated session that already exists for that address. A smaller inactivity time reduces the chance of this event happening.

Authentication Proxy Sample Configuration

```
aaa new-model
aaa group server radius authproxy
 server-private <ip address> auth-port 1812 acct-port 1813 key 0 <key>
 ip radius source-interface Vlan10
!
aaa authorization auth-proxy default group authproxy
!
ip inspect fw test tcp
ip inspect fw test udp
ip inspect fw test rtsp
ip inspect fw test tftp
ip inspect fw test skinny
ip inspect name test sip
ip inspect name test sip-tls
!
ip admission auth-proxy-banner file http://10.34.250.98/disclaimer.htm
ip admission auth-proxy-banner http ^
This is the authentication proxy challenge
^
ip admission max-login-attempts 6
! Configure 30 minutes of inactivity timeout.
! proxy_acl is the intercept ACL
ip admission name pxy proxy http inactivity-time 30 list proxy_acl
!
ip admission name test_proxy proxy http list proxy_acl
interface Vlan10
 description inside interface
 ip inspect fw in
 ip access-group proxy_inbound_acl in
 ip admission test_proxy
 !...
ip access-list extended proxy_acl
 remark --- Auth-Proxy ACL -----------
 ! Deny lines are used to bypass auth-proxy
 deny  tcp any host 10.10.200.1 eq www
 ! auth-proxy will intercept http access matching the below permit lines
```

```
 permit tcp any 10.10.30.0 0.0.255 eq www
 …
!
ip access-list extended proxy_inbound_acl
 remark --- Auth-Proxy Inbound ACL which blocks the traffic ---
 ! Allow access to certain protcols
 permit udp any any eq domain
 permit udp any any eq netbios-ns
 permit udp any any eq netbios-dgm
 permit udp any any eq 5445
 permit tcp any any eq 5060
 permit tcp any any eq 5061
 permit tcp any any eq 2000
 permit tcp any any eq 2443
 permit udp any any eq tftp
 ! Block corporate subnets. If split tunneling is not enabled denying
 ! all traffic using
 ! “deny any any” is sufficient
 deny  ip any 10.0.0.0 0.255.255.255
 …
 …
 Permit ip any any ! if split tunneling is enabled
!
```

IP Phone Consideration

IP phones cannot display the Authentication Proxy prompt, so they cannot be authenticated using AuthProxy. One solution to this problem is to use Context-Based Access Control (CBAC). IP phones usually download their initial configuration using Trivial File Transfer Protocol (TFTP). In that case TFTP needs to be opened in the inbound ACL. If the IP phone is using Skinny Client Control Protocol (SCCP), then User Datagram Protocol (UDP) port 2000 needs to be opened. IP inspection dynamically opens holes for Real-Time Transport Protocol (RTP) streams when a phone call is made. By opening only UDP 2000, access control is not diluted much and the IP phone works without doing AuthProxy. The same thing works for Session Initiation Protocol (SIP) phones, but for SIP phones you need to open UDP ports 5060 and 5061.

UDP port 5445 needs to be opened if Cisco Unified Video Advantage (CUVA) is enabled on the IP phone.

Table 1 lists some important Authentication Proxy diagnostics commands.

Table 1. Authentication Proxy Diagnostics Commands

`show ip auth-proxy cache`	Displays the existing AuthProxy sessions
`show ip auth-proxy config`	Displays the current configuration
`clear ip auth-proxy cache [*/<ip address>]`	Clears AuthProxy sessions
`debug ip auth-proxy [options]`	Enables AuthProxy debugs

IEEE 802.1x-Based Device Authentication

Using IEEE 802.1x-based device authentication, all IP devices connecting to the router are subject to 802.1x-based credential validation. This authentication works only on the switch ports of the integrated services router platforms. The device does not get an IP address until the credentials are validated. When validated, the port becomes active and the device gets network access. If the validation fails the port is shut down.

This authentication requires an 802.1x client (called supplicant) running on the device. Many devices such as IP phones do not have an 802.1x supplicant. In order to accommodate client less device, guest VLAN feature can be enabled. Guest VLANs typically have less access privilege than the primary VLAN. In the case of Cisco Virtual Office, the guest VLAN is part of VLAN20.

Cisco IP phones can request a voice VLAN. If a voice VLAN is enabled on the router, the Cisco IP phone is automatically placed in that VLAN and bypasses 802.1x authentication.

If just user authentication is the goal, then AuthProxy is sufficient. Table 2 compares Authentication Proxy and 802.1x authentication.

Table 2. Authentication Proxy vs. 802.1x

	Authentication Proxy	802.1x
Protocol used	HTTP—Can be configured on any router on the network path.	IEEE 802.1x:—Should be configured on the immediate networking device (spoke router on CVO). Even if there is a switch or a wireless access point between the device and the router, 802.1x will not work because those devices consume or discard 802.1x frames. Therefore, the inside network can be expanded only by using a hub.
Client type	A web browser: Any device with a web browser can authenticate.	802.1x supplicant: Only those devices with a supplicant can authenticate.
Access control Mechanism	Permit ACEs are downloaded (Cisco attribute-value [AV] pair configured on RADIUS server) for an authenticated device. Nothing happens for an unauthenticated device.	Authenticated devices are associated with a trusted VLAN and unauthenticated ones are associated with a guest VLAN (or blocked). Separate access control, firewall, and Network Address Translation (NAT) polices for each VLAN.
Split Tunneling Concern	If **no-split tunneling** is configured, unauthenticated devices may not get network access.	If **no-split tunneling** is configured, unauthenticated devices can still be given access to the public Internet because separate NAT and firewall polices can be applied to the unauthenticated devices without sacrificing overall security.
Role-Based Access	The usernames can belong to different groups on the RADIUS server, and different ACEs can be downloaded for users depending on which group that user belongs to.	There are only two classifications: trusted and nontrusted.

For more information about this feature and its configuration on Cisco Virtual Office, refer to the deployment guide “Deploying 802.1x-Based Port Authentication on the Cisco Virtual Office Solution” (Reference 6). All the Cisco Virtual Office deployment guides are available at http://www.cisco.com/go/cvo.

Secure ARP

Secure Address Resolution Protocol (ARP) locks the Dynamic Host Configuration Protocol (DHCP)-assigned IP address to a MAC address. The DHCP server does not reassign this IP address to another device unless it has received a DHCP release. During an active lease a different IP address cannot overwrite the ARP entry, reducing the possibility of IP address spoofing. With this setup a second computer cannot take control of the IP address by manually configuring it on the interface.

Secure ARP Configuration

```
ip dhcp pool client
 update arp
```

Router Security and Authentication

It is assumed that the router at a remote office or home office has a certain level of physical security. But it is not as safe as sitting inside an office building where the access is limited to only employees. The following features add some extra security to the routers to compensate.

RSA Keys and Certificates

The routers are configured with RSA key pairs for the purpose of VPN. Digital certificates are issued to each router. Digital certificates are very difficult to spoof. Because the certificates are used for PKI authentication, no unauthorized spokes are connected to the VPN. Unless marked as exportable, the RSA keys cannot be exported, meaning that RSA keys cannot be transferred to another router. Cisco IOS Software supports certificate servers from many vendors, including one based on Cisco IOS Software.

Following is the basic configuration of the PKI feature. For more details about the configuration and deployment options, refer to the deployment guide “Public Key Infrastructure Integration with Cisco Virtual Office Solution“ (Reference 8) and “Public Key Infrastructure Resource Page” (Reference 9).

Certificate Authority Trustpoint Configuration

The following sample configuration uses a Cisco IOS Software certificate server.

```
ip host test-ca <ip address>
crypto pki trustpoint testtp
 enrollment url http://test-ca:80
 ! Include serial number in the certificate request
 serial-number
 ! Do not check CRL for peer certificates
 revocation-check none
 ! Source the traffic from Vlan10 for any communication with
 ! Cert server
 source interface Vlan10
 ! Re-enroll automatically when the current cert is 75% of its age
 auto-enroll 75
```

Generating RSA Keys

The following command is executed in configuration mode:

```
crypto key gen rsa general-keys modulus 1024
! Refer the documentation guide for other options.
```

Authenticating the Certificate Authority Server

The following command is executed in configuration mode. The Certificate Authority server root certificate is downloaded as a result of this command:

```
crypto pki authenticate test-ca
```

Enrolling with the New Certificate Authority Server

This feature is also executed in configuration mode. After execution the router gets its public key signed by the Certificate Authority server, generating its certificate.

```
cry pki enroll test-ca
```

Conditional CRL Checking

In some cases there might be a need to skip Certificate Revocation List (CRL) checking for some peer routers; Cisco Virtual Office is an example. In the Cisco Virtual Office solution, if the CRL is hosted on the management network, the spoke router cannot download the CRL without first establishing the management VPN tunnel. So the CRL checking needs to be skipped when establishing the management VPN tunnel. All future VPN establishment with other hubs and spokes will continue to check CRL after it is downloaded though the management tunnel.

The following configuration example skips CRL validation for a peer certificate if the subject-name of the certificate contains “mgmthub1.mydomain.com” or “mgmthub2.mydomain.com”:

```
crypto pki trustpoint testtp
 …
 revocation-check crl
 match certificate mgmt-hub skip revocation-check
!
crypto pki certificate map mgmt-hub 1
 subject-name co mgmt-hub1.mydomain.com
crypto pki certificate map mgmt-hub 2
 subject-name co mgmt-hub2.mydomain.com
```

Note: Instead of subject-name, other fields in the certificate can also be matched in the rule. The **match certificate …** command has other options also, but they are not discussed in this document.

Table 3 lists some important diagnostic and show commands for PKI.

Table 3. Diagnostic and Show Commands for PKI

`show crypto pki certificates`	Displays the certificate details of the router: The certificate with title “Certificate” is issued to the router. The certificate titled “CA certificate” belongs to the Certificate Authority, which is also called the root certificate. A good certificate should have status “Available”.
`show crypto pki trustpoints`	Displays the trustpoint details
`debug crypto pki transactions`	Provides the basic debugging needed to diagnose the certificate authentication, enrollment, and validation problems
`debug crypto pki messages`	Provides some more detailed debugs

PKI-AAA Authentication and Authorization

The hub router can be configured to do certificate revocation list (CRL) validation for each peer certificate. PKI-AAA authorization is an alternative way to validate the peer certificates. This authorization can also work as an additional check along with CRL validation. The router extracts a specified field from the peer certificate subject and sends it to a RADIUS server. It is sent as the username, and the password is fixed as “cisco”. The field that should be sent as the username is specified in the trustpoint configuration.

If the RADIUS server has an entry for this username with password set as “cisco”, the query returns success along with the following Cisco attribute-value (AV) pairs configured for that username:

- Certificate usage (cert-application)
- Certificate trustpoint (cert-trustpoint)
- Serial number (cert-serial)
- Certificate lifetime (cert-lifetime-end)

Following is a sample Cisco AV pair configuration which can be configured on a Cisco Secure Access Control Server (ACS):

```
cisco-avpair = “pki:cert-application=all”
cisco-avpair = “pki:cert-trustpoint=msca”
cisco-avpair = “pki:cert-serial=16318DB7000100001671”
cisco-avpair = “pki:cert-lifetime-end=1:00 jan 1, 2003”
```

The RADIUS server returns failure if the record is not found or password is not “cisco”. The peer certificate is not accepted if the RADIUS request failed.

Among these AV pairs only cert-application is mandatory. If this AV pair is not returned or the value of the AV pair is “none”, then the certificate is rejected. For the certificate to be accepted, the value of the cert-application should be “all” (more specific keyswords may be supported in the future; “all” means the certificate can be used for any purpose, including PKI).

If any or both of “cert-trustpoint” and “cert-serial” are specified, the router compares these values with the trustpoint name and serial number extracted from the peer certificate. The certificate is accepted only if these fields match.

The ”cert-lifetime-end” value can be used to bypass the actual expiry date of the certificate. This is useful if an expired peer certificate needs to be accepted. A different date can be specified in the AV pair and the router will use this date for the expiry date calculation.

With the PKI-AAA feature the hub accepts a certificate only if it has an entry on the RADIUS server. The certificate can be temporarily disabled by setting the “cert-application” value to “none.”

PKI-AAA Configuration

```
aaa new-model
aaa group server radius pki-aaa-server
 server <ip addr> auth-port 1812 acct-port 1813
!
aaa authorization network pkiaaa group pki-aaa-server
!
```

```
crypto pki trustpoint testtp
 enrollment mode ra
 enrollment url http://test-ca:80/certsrv/mscep/mscep.dll
 authorization list pkiaaa
 authorization username subjectname commonname
```

Diagnostics

Use **debug crypto pki transactions** regular AAA and RADIUS debugs to diagnose problems. The logs on the RADIUS server also help.

For more details about this feature, refer to the deployment guide “Public Key Infrastructure Integration with Cisco Virtual Office Solution” (Reference 8).

RSA Key Erase on Password Recovery

The spoke routers are centrally managed. Therefore there is no need for the end user to know the router administrator password. If any user tries to do a password recovery, then the RSA key becomes un-usable. The password recovery process involves booting the router without loading the router configuration and then copying the startup configuration to the running configuration. During this process, the RSA private key is not copied to the running configuration. Without the private key the router cannot establish the VPN session. If the user issues a **write mem** command at this point, the RSA private key will be permanently lost . User will have to contact the administrator to restore VPN connectivity.

This feature does not have any specific configurations. It is enabled by default and cannot be disabled.

RSA Key Locking

This feature locks the RSA key using the specified password. When locked, it needs to be unlocked before it can be used for negotiating VPN sessions. The key is automatically locked after a reboot. This feature is useful if the router is to be installed in insecure places or needs to be shipped fully configured. If the router is stolen, it cannot be used to establish VPN connectivity to the corporate network without giving the correct unlock password. If the router falls into the wrong hands, this feature acts as a deterrent from getting illegal access to the corporate VPN.

Generating an RSA Key Pair

```
test-router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys is test-router.cisco.com.
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
test-router(config)#
```

Encrypting the RSA Key

```
test-router(config)#crypto key encrypt rsa passphrase <pass-phase>
Encrypting keypair labeled test-router.cisco.com
WARNING: Configuration with encrypted key not saved.
 Please save it manually as soon as possible to
 save encrypted key
test-router(config)#
```

Now the key is encrypted. The output of **sh cry key my rsa** will have the string “*** The key is protected and UNLOCKED. ***”.

Locking the RSA Key

```
test-router>crypto key lock rsa passphrase <pass-phase>
```

Now the key is locked. The output of **sh cry key my rsa** will have the string "*** The key is protected and LOCKED. ***".

Unlocking the RSA Key

```
test-router>crypto key unlock rsa passphrase <pass-phase>
```

If there are more than one set of keys on the router, the administrator can selectively lock or unlock by specifying the name of the set in the command line.

```
crypto key encrypt rsa name <key name> passphrase <pass-phrase>
```

The user can also use the web interface to unlock the RSA key by accessing the URL http://<router's ip address>/exec/crypto/key. Only privilege 1 users can lock or unlock the RSA key. Administrators can create a privilege 1 user account on the router to give other users lock and unlock privileges; the process is accomplished by accessing the URL http://<router's ip address>/level/01/exec/crypto/key/.

```
user <username> priv 1 pass <password>
ip http server
ip http authentication local
```

Diagnostics

```
show crypto key mypubkey rsa—Displays the RSA key status.
```

Disabling Password Recovery

The Cisco IOS Software router provides the facility to recover from a forgotten password. An IOS savvy end user may be able to look at the router configuration using this method. This can be prevented by disabling password recovery. To prevent unwanted password activity, **no service password-recovery** can be configured on the router:

```
config terminal
test-router(config)#no service password-recovery
WARNING:
Executing this command will disable password recovery mechanism.
Do not execute this command without another plan for password
recovery.
Are you sure you want to continue? [yes/no]:yes
test-router(config)#
```

Restricting Console Access

The security policy of some customers may require controlling access to the console port. There are two ways to control the console access, password protection and locking down.

If console access authentication is enabled, the console access is password-protected. User will be prompted for username and password. Access is granted only if the correct credentials are entered. The router can be configured to verify with the local credentials configured on the router or with a RADIUS or TACACS server. Doing local authentication will ensure that console access is possible even if the network connectivity is down.

Configuration for Local Authentication

```
aaa authentication login default local
username <username> password <password>
!
```

Configuration for RADIUS-Based Authentication

```
aaa group server radius myradius
 server-private 10.32.227.161 auth-port 1812 acct-port 1813 key
<server password>
!
aaa authentication login default group myradius
! “aaa authentication login default local group myradius” will check
! with both local and RADIUS user database.
```

Disabling Console Access

Disabling console access completely locks down the console. When this feature is enabled, the only way to access the router is by using network-based mechanisms such as Secure Shell (SSH) Protocol or Telnet. When the network access is gone, the router is inaccessible. Therefore, extreme caution should be exercised when deploying this feature on the router. For example, if the user changes his ISP to a different IP address assignment , the router may not be accessible via the network anymore. The user needs to press the reset button on the Cisco 881 router platform for 6 to 10 seconds while the router is rebooting to reset the router to the factory default configuration.

Configuration for Locking the Console Port

```
menu disable clear-screen
menu disable title %Console Disabled%
line con 0
 autocommand menu disable
! “clear line 0” will clear the console connection if a connection
! is active. But this needs to be done from a ssh or telnet window.
```

Network Security

Stateful Firewall—Legacy Configuration

The spoke router and the network behind the spoke should be considered as part of the corporate network. So an attempt should be made to provide the same level of security as for the corporate firewall.

An access list is configured on the outside interface (which is connected to the ISP) such that no traffic initiated from outside (Internet) is permitted into the network. Only VPN traffic and some basic traffic such as Internet Control Message Protocol (ICMP), DHCP, Network Time Protocol (NTP), and so on are permitted into the router.

Port Address Translation (PAT) is configured on the outside interface such that all traffic originated from inside the network to the Internet is translated into a single public IP address. PAT is configured so that multiple devices behind the router can share the same IP address assigned by the ISP.

IP inspection (CBAC) is configured on the inside interface. When traffic is originated from inside toward the public network, CBAC selectively opens holes in the firewall ACL for the return traffic.

CBAC and PAT are needed on the spoke router only if Split Tunneling is allowed. Otherwise all traffic is directed through the corporate network. No firewall or address translation is configured between the corporate network and the trusted network (which is the tunnel interface).

Stateful Firewall Configuration

```
ip inspect name fw tcp
ip inspect name fw udp
ip inspect name fw realaudio
ip inspect name fw rtsp
ip inspect name fw tftp
ip inspect name fw ftp
ip inspect name fw h323
ip inspect name fw smtp
ip inspect name fw skinny
ip inspect name fw sip
!
interface Vlan10
 description inside interface – Secure network with corporate access
 ip address 10.10.100.1 255.255.255.240
 ip nat inside
 ip inspect fw in
!
interface Vlan20
 description inside interface – Gust network without corporate access
 ip address 10.10.200.1 255.255.255.240
 ip nat inside
 ip inspect fw in
!
interface FastEthernet4
 description outside interface
 ip address dhcp
 ip access-group fw_acl in
 ip nat outside
!
ip nat inside source list nat_acl interface Fastethernet4 overload
ip access-list extended nat_acl
 permit ip 10.100.100.0 0.0.0.15 any
 permit ip 10.100.200.0 0.0.0.15 any
!
```

Table 4 gives firewall diagnostics.

Table 4. Firewall Diagnostics

`show ip inspect sessions`	Displays active inspect sessions
`show ip inspect sessions detail`	Displays details of the active sessions: Use this command to display the temporary ACEs installed on the firewall ACL for each flow.
`show ip inspect config`	Displays the configuration details
`debug ip inspect detail`	Shows details of IP inspect debugging
`debug ip inspect <protocol>`	Performs protocol-specific (TCP, UDP, Skinny Client Control Protocol, etc.) inspect debugging
`show ip nat translations`	Displays the active NAT translations
`show ip nat statistics`	Displays NAT statistics
`debug ip nat detailed`	Shows details of NAT debugging
`show ip access-lists <firewall ACL name>`	Displays access list with hit count for each line
`clear ip access-list counters`	Clears the access-list hit counters: A “log” keyword can be added to an ACE, which needs more debugging. This will generate a log message when there is a traffic match for that line. Use this only for debugging, as this causes performance degradation.

Intrusion Prevention System

An intrusion prevention system (IPS) alerts the network administrator about attacks on the network in real time. The traffic is inspected for known signatures, and if any are detected, alerts are generated. Alerts can be captured on a syslog server or a management tool with the appropriate support. Apart from detecting an attack, it can also block many of the attacks.

IPS is configured globally on the router and then applied on the necessary interfaces. The traffic can be inspected in any direction which is configurable.

The IPS signatures are periodically published on Cisco.com. These signature files need to be downloaded to IOS router periodically so that IPS signature set is up-to-date. Automatic signatures updates are possible either by using the Cisco IOS IPS automatic update feature or by using a management tool which supports pushing signatures to Cisco IOS Software routers.

Note: IPS 4.x is not compatible with Cisco IOS Software Release 12.4(11)T and later. When upgrading to 12.4(11)T or later, the old IPS configuration needs to be removed and replaced with new configuration. The signature format is also different in IPS 5.x.

IPS 5.x can be enabled with five basic steps:

Step 1. Download the latest signature file and public key file from Cisco.com and host the signature file in a local TFTP server. The public key needs to be setup only once. Signature file can be updated as and when new signature files appear on Cisco.com. A valid Cisco.com account is needed to download the files.

- To access files: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup
- Signature file: IOS-Sxxx-CLI.pkg, where xxx is the version number; choose the latest version
- Public key file: realm-cisco.pub.key.txt

Step 2. Create a directory on the router flash memory to save the IPS signatures.

- At the enable prompt type “cd flash:/” and press <RETURN> key. “dir” command can be used to check the current directory. (On some IOS platforms primary disk space may not be called “flash”. In that case use the appropriate the disk name.)
- Execute **mkdir ipsstore** at the enable prompt. A directory named “ipsstore” will be created now. Use the **dir** command to verify.

```
myrouter#cd flash:/
myrouter#
myrouter#mkdir ipsstore
Create directory filename [ipsstore]?
Created dir flash:ipsstore
myrouter#
myrouter#dir
Directory of flash:/

    2  -rwx    18850232  Dec 12 2007 20:39:48 -08:00  c870-
advipservicesk9-mz.124-15.T1
    3  drwx         384  Dec 21 2007 18:15:55 -08:00  ipsstore

52383744 bytes total (9826304 bytes free)
myrouter#
```

Step 3. Configure the Cisco IOS IPS cryptographic public key.

At the enable prompt, go to the configuration mode by executing **config terminal**. At the configuration prompt, copy and paste the contents of the file “realm-cisco.pub.key.txt” that was downloaded at step 1. This step will configure the IPS public key on the router. Save the router configuration.

```
myrouter#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
myrouter(config)#crypto key pubkey-chain rsa
myrouter(config-pubkey-chain)# named-key realm-cisco.pub signature
Translating "realm-cisco.pub"...domain server (171.68.226.120)
myrouter(config-pubkey-key)#  key-string
Enter a public key as a hexidecimal number ....

myrouter(config-pubkey)# F70D0101 01050003 82010F00 3082010A 02820101
..
<paste the whole key string here and end with “quit” in a newline>
..
myrouter(config-pubkey)# F3020301 0001
myrouter(config-pubkey)# quit
myrouter(config-pubkey-key)# exit
myrouter(config-pubkey-chain)# exit
myrouter(config)#end
myrouter#
```

Step 4. Configure Cisco IOS IPS on the router.

The following example enables the basic Cisco IOS IPS signature category and specifies the mitigation action for the detected signatures. Two signature categories exist for Cisco IOS IPS, basic and advanced. Enabling the advanced signature set may affect performance on low-end platforms such as the Cisco 881.

```
! Create the IPS rule name.
ip ips name ips5
! Configure the signature storage location
ip ips config location flash:ipsstore
! Configure the report notification method. SDEE or log (for syslog)
! are supported.
ip ips notify SDEE
! Enable the basic signature set.
ip ips signature-category
  category all
   ! Disable the full signature category.
   retired true
  category ios_ips basic
   ! Enable the “basic” category.
   retired false
   ! Configure TCP reset and traffic blocking as the mitigation
   ! actions for this category.
   event-action reset-tcp-connection deny-packet-inline
!
! Enable the IPS policy on the desired interfaces. On ECT spoke
! router IPS is enabled on the traffic from Trusted network to
! corporate network. It can also be enabled on other interfaces
! to inspect more traffic.
!
interface Vlan10
 ! Enable IPS on incoming traffic.
 ip ips ips5 in
 end
! Save the configuration by doing “write mem”.
```

Step 5. Load the signatures to the router. This step is done at the enable prompt. This step is the final step, and it is repeated whenever a new signature set is available that you need to load.

```
myrouter# copy tftp://<ip address of tftp server>/IOS-S312-CLI.pkg
idconf
Loading stealth/IOS-S312-CLI.pkg from <ip address>  (via Tunnel13):
!!OO!!!!!!!!!!!!!!O!!!!!!!!!!!!!!
[OK–7686949 bytes]
```

Refer to the “Cisco IOS Software IPS resource page” (Reference 12) for design considerations and best practices. “Getting Started with Cisco IOS IPS with 5.x Format Signatures” (Reference 14) describes IPS 5.0 deployment in more detail.

Automatic Signature Update

The Automatic Signature Update feature is used if the signature is periodically downloaded from Cisco.com and saved in a fixed location and with the same name. It can be configured to be retrievable over TFTP, FTP or HTTP. In the following example, the signature is loaded once daily using TFTP.

User has the flexibility of configuring the minute of the hour, the hours of the day (one: 2; many: 1,2,4; and range: 1–24), days of the month (one, many, or range) and days of the week (one, many, or range) at which the automatic update should occur.

```
ip ips auto-update
 ! Do update at 1:00 am on every day of the month
 occur-at 0 1 1-31 0-6
 url tftp://mytftpserver/ipstore/signature.xml
```

Table 5 gives the Cisco IOS IPS diagnostics.

Table 5. Cisco IOS IPS Diagnostics

`show ip ips all`	Displays all the basic IPS details
`show ip ips configuration`	Shows IPS configuration details
`show ip ips signatures`	Shows IPS signature details
`show ip ips statistics`	Shows some IPS statistics
`debug ip ips sessions`	Displays the traffic flows inspected by IPS
`sh ip ips auto-update`	Displays the status of Automatic Signature Update

Split DNS

The Split DNS feature helps enable a Cisco router to respond to DNS queries based on certain characteristics of the queries. In a Split DNS environment, multiple DNS databases can be configured on the router, and the Cisco IOS software can be configured to choose one of these DNS name server configurations whenever the router must respond to a DNS query by forwarding or resolving the query.

This feature is useful in Cisco Virtual Office when Split Tunneling is enabled. When Split DNS is configured, end hosts send the DNS queries to the router, which forwards the DNS requests to the appropriate DNS server; the reply is relayed back to the end host. DNS resolution for corporate hosts is resolved by corporate DNS servers, and the noncorporate queries are resolved by noncorporate DNS servers (for example, ISP DNS servers).

Refer to the Split DNS user guide (Reference 20) for more details.

Split DNS Configuration

The Cisco Virtual Office configuration needs to be modified as follows:

```
ip dhcp pool client
    dns-server <ip address of Vlan10>
!
ip dns view resolve-corporate
 domain name mycompany.com
 dns forwarder <corporate DNS server1>
 dns forwarder <corporate DNS server2>
```

```
 dns forwarding source-interface Vlan10
ip dns view resolve-internet
 dns forwarder <ISP DNS server 1>
 dns forwarder <ISP DNS server2>
 dns forwarding source-interface Vlan10
ip dns view-list dns-list
  ! Corporate rule will be checked first
 view resolve-corporate 3
  restrict name-group 10
 view resolve-internet 5
  restrict name-group 20
ip dns name-list 10 deny www.mycompany.com
ip dns name-list 10 deny ftp.mycompany.com
ip dns name-list 10 permit .*.mycompany.com
ip dns name-list 20 permit .*
ip dns server
!
interface Vlan10
 ip dns view-group dns-list
!
! Legacy firewall
ip access-list extended fw_acl
 permit udp any eq domain any
! Zone based firewall
! Access list for self2net_policy needs to be modified to allow DNS
traffic
ip access-list extended outbound_acl
  permit udp any eq domain any
!
```

Table 6 gives Split DNS diagnostics.

Table 6. Split DNS Diagnostics

`show ip dns statistics`	Displays the DNS statistics
`show ip dns view-list`	Lists the DNS views
`show ip dns view`	Displays the DNS configuration
`show ip dns name-list`	Lists the DNS name lists

Hardware and Software Details

This deployment guide is based on a Cisco 881 Integrated Services Router running Cisco IOS Software Release 12.4(20)T.

References

1. Cisco Virtual Office Deployment Guide: http://www.cisco.com/application/pdf/en/us/guest/tech/tk372/c1550/cdccont_0900aecd801dc5b2.pdf
2. Cisco IOS Software DMVPN: http://www.cisco.com/go/dmvpn
3. Cisco IOS Software IPsec: http://www.cisco.com/go/ipsec
4. Authentication Proxy Authentication Outbound-No Cisco IOS Firewall or NAT Configuration: http://www/en/US/partner/products/sw/secursw/ps1018/products_configuration_example09186a00800942fd.shtml
5. Implementing Authentication Proxy: http://www.cisco.com/warp/public/793/ios_fw/auth_intro.html
6. Deploying 802.1x-Based Port Authentication on the Cisco Virtual Office Solution: http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd805a5ab5.shtml
7. Cisco IOS Software 802.1x information: http://www.cisco.com/warp/public/732/Tech/security/trust/8021x/
8. Public Key Infrastructure Integration with Cisco Virtual Office Solution: http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd805249e3.shtml
9. Public Key Infrastructure resource page: http://www.cisco.com/warp/public/732/Tech/security/trust/pki/
10. Zone-Based Policy Firewall Design and Application Guide: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml
11. Cisco IOS Firewall resource page: http://www.cisco.com/go/firewall
12. Cisco IOS Software IPS resource page: http://www.cisco.com/go/iosips
13. IPS 5.x Signature Format Support and Usability Enhancements: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ips_v5.html
14. Getting Started with Cisco IOS IPS with 5.x Format Signatures http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd805c4ea8.shtml
15. Cisco Secure ACS for Windows documentation page: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm
16. Cisco IOS Software documentation page: http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm
17. Cisco IOS Software infrastructure security: http://www.cisco.com/go/infrastructure
18. Cisco IOS Software AutoSecure: http://www.cisco.com/go/autosecure
19. Cisco integrated services routers: http://www.cisco.com/go/isr
20. Split DNS user guide: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htspldns.html
21. Advanced Layered Security Features on Cisco Virtual Office guide:

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-493576-00 08/08