Deployment Guide

Cisco Virtual Office: Advanced Layered Security

Contents

Scope of Document **3**

Introduction **3**

Platforms and Images **3**

Network Security **3**

Stateful Firewall—Traditional Configuration 3
Zone-Based Policy Firewall 5
Intrusion Prevention System 13
Automatic Signature Update 16
Split DNS 16
Object Group-Based ACLs 17

Router Security and Authentication **20**

RSA Keys and Certificates 20
RSA Key Erase on Password Recovery 23
RSA Key Locking 23
Disabling Password Recovery 24
Restricting Console Access 24
Disabling Console Access 25

User and Device Security and Authentication **25**

Authentication Proxy 25
802.1x-Based Device Authentication 28
User Group Firewall 33
Secure ARP 40

References **41**

Scope of Document

This deployment guide provides detailed design and implementation information for deployment of Layered Security features with 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.

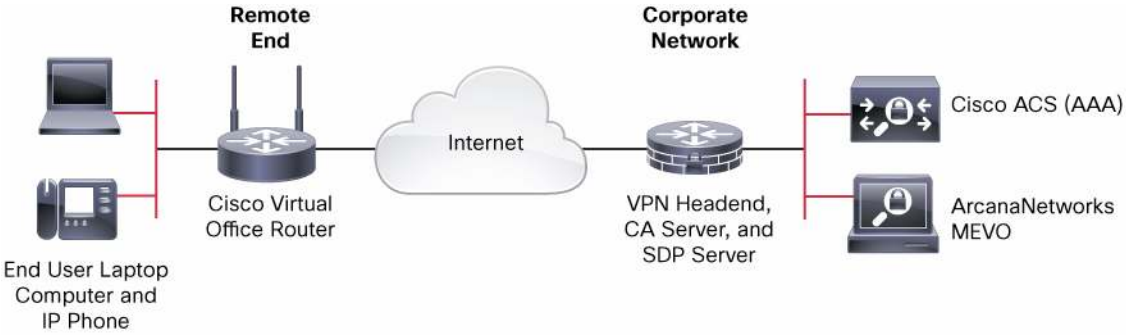
Introduction

This guide assumes basic knowledge about the Cisco® Virtual Office deployment solution and basic Layered Security features. For more information about the Cisco Virtual Office solution, please visit the official Cisco Virtual Office site at http://www.cisco.com/go/cvo.

Platforms and Images

Sample configurations and screenshots in this guide are based on the Cisco 881 Integrated Services Router with wireless running Cisco IOS® Software Release 15.1(1)T. The FastEthernet4 interface connects to the Internet service provider (ISP). For other Cisco router platforms, the sample configurations may require minor modifications. Technologies discussed in this document are applicable to the remote end router in the Cisco Virutal Office topology (Figure 1).

Figure 1. Cisco Virutal Office Topology



For a complete list of supported and recommended platforms and images, please refer to Cisco Virtual Office Supported Hardware and Software at http://www.cisco.com/go/cvo.

Network Security

Two internal networks are configured using VLANs, namely VLAN10 and VLAN20. They are called ”trusted” network and “guest” network, respectively, 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.

Stateful Firewall—Traditional Configuration

The spoke router and the network behind the spoke router should be considered as part of the corporate network, so the same level of security as for the corporate firewall should be provided.

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 trusted VLAN of 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 1 provides some firewall diagnostic commands.

Table 1. Firewall Diagnostics

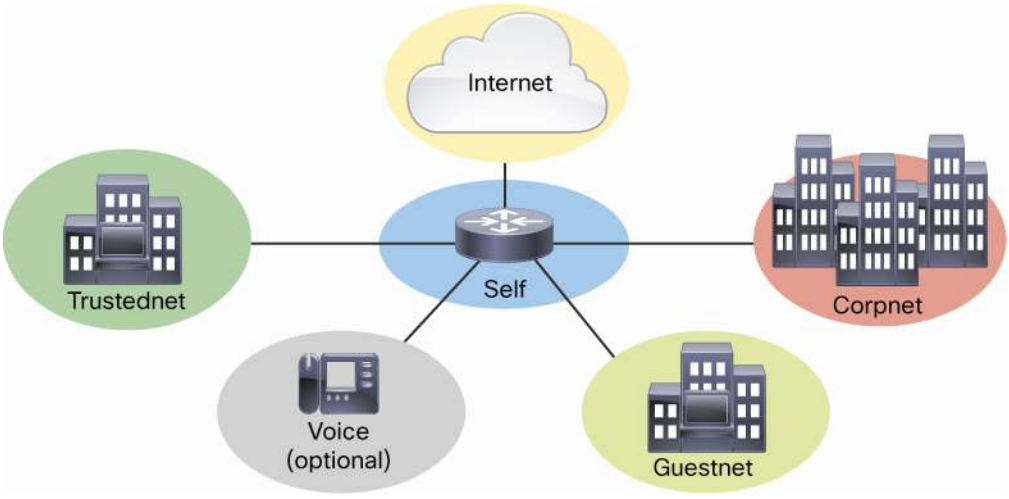
show ip inspect sessions	Displays active inspect sessions
show ip inspect sessions detail	Displays details of the active sessions: Use this command to display the temporary ACEs installed on the firewall ACL for each flow.
show ip inspect config	Displays the configuration details
debug ip inspect detail	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 that needs more debugging. This keyword will generate a log message when there is a traffic match for that line. Use this keyword only for debugging, because it causes performance degradation.

Zone-Based Policy Firewall

Zone-Based Policy Firewall (ZFW) is an alternative way to configure and deploy firewall policies. This new configuration model offers intuitive policies for multiple-interface routers, increased granularity and flexibility of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic. Certain features also require Zone-Based Policy Firewall to be configured in order to be used.

In Zone-Based Policy Firewall, multiple security zones are defined. Each zone has different network privileges. Each router interface is configured to be part of one of the zones. The traffic flow is unrestricted between interfaces belonging to same zone, but traffic flow between two different zones is blocked unless an access policy is defined between them. In traditional firewall, the policies are applied on the interface itself, whereas in zone-based firewall they are applied between the zones (Figure 2).

Figure 2. Zones in a Typical Cisco Virtual Office Deployment



The Zone-Based Policy Firewall configuration is done using Cisco Policy Language. Following are the basic design steps to take before finalizing the firewall configuration:

- **Identify zones:** Identify interfaces that should have the same access privileges and group them in zones.
- **Identify zone pairs**: Identify all the zone pairs between which traffic flow needs to be allowed. If a zone pair is not defined, traffic will not be allowed between them by default.
- **Create traffic policy:** Identify the traffic restrictions between each identified zone pair and define them as Cisco Policy Language policies.
- Finally, attach the policy to a zone pair.

Primarily three Cisco Policy Language constructs are used for defining a Zone-Based Policy Firewall policy:

- **Class-map:** To specify interesting traffic through “match” conditions
- **Policy-map:** To associate actions with the traffic specified by the class map.
- **Parameter-map:** Any operating parameters needed for the actions of class or policy mapping

For more details about Zone-Based Policy Firewall, refer to the Zone-Based Policy Firewall Design Guide at http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml.

Four network zones are defined on a Cisco Virtual Office spoke router:

- **Corpnet:** Zone connecting to corporate network, typically the tunnel interface
- **Internet:** Zone connecting to Internet connection
- **Trustednet:** Zone where the IP devices at home are connected; this zone needs to have corporate access
- **Guestnet:** Zone where other nonemployee devices are connected; this zone has no corporate access (only Internet)

Apart from the user-defined zones, there is also a hidden zone named “self”, which is defined for the traffic consumed by the router itself. Traffic is allowed by default between any zone and the self zone.

Following are the important zone pairs and the traffic policies between them:

- **Trustednet to Internet:** Enable Context-Based Access Control (CBAC) so that the return traffic is permitted.
- **Trustednet to corpnet:** All traffic is allowed to the corporate network.
- **Trustednet to guestnet:** Enable CBAC. From the perspective of the trustednet, the guestnet has the same Internet privileges.
- **Corpnet to trustednet:** All traffic is allowed.
- **Internet to trustednet:** Block all traffic by default; CBAC permits the return traffic corresponding to the trustednet-to-Internet traffic.
- **Guestnet to Internet:** Enable CBAC, so that return traffic is allowed in the reverse direction.
- **Self to Internet:** Allow all traffic.
- **Internet to self:** Allow only restricted traffic (such as VPN, management network, etc.).

All other zone pairs not listed (and not including the self zone) assume the default policy of not allowing any traffic between them.

ZFW Design Considerations

The following are some of the design considerations to keep in mind while designing a ZFW policy:

- If no policy is defined, traffic between any two security zones is dropped.
- If no policy is defined, traffic between any zone and the self zone is permitted (except in some cases; refer to the next bullet). This setup helps to maintain the network access to the router while ZFW polices are applied to the router, so you should define a strict access policy between security zones and the self-zone—especially between untrusted zones and the self zone.
- Sometimes the router-originated traffic is configured to use the IP address of a different interface than the outgoing interface as the source IP address of the traffic. In that case, the outgoing traffic follows the zone-to-zone policy between the zones, instead of the self-zone policy described in the previous bullet. Incoming traffic destined to the router still follows the zone-to-self-zone policy, even if the destination IP address is different from the address of the incoming interface.
- Application firewall inspection between the self zone and the security zone is not as comprehensive as the zone-to-zone inspection.
- For more design considerations, refer to the Zone-Based Policy Firewall Design and Application Guide at http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml.

Zone-Based Firewall Configuration

```
! Traffic class definitions
class-map type inspect match-any inspect_protocols
 match protocol dns
 match protocol smtp extended
 match protocol rtsp
 match protocol tftp
 match protocol h323
 match protocol skinny
 match protocol sip
 match protocol sip-tls
 match protocol realmedia
 match protocol streamworks
 match protocol tcp
 match protocol udp
 match protocol icmp
!
class-map type inspect match-any edge_fw
 match access-group name fw_acl
 match access-group name fw_mgmt_acl
class-map type inspect match-any mgmt_traffic
 match access-group name mgmt_acl
class-map type inspect match-any outbound_traffic
 match access-group name outbound_acl
!
```

```
! Policy definitions
! Do CBAC inspect on the matching traffic going to Internet. Drop the
! un-matched traffic
policy-map type inspect trusted2net_policy
 class type inspect inspect_protocols
  inspect
 class class-default
  drop
! This policy permits all traffic
policy-map type inspect pass_all_policy
 class class-default
  pass
! In this example trusted to guest policy is same as trusted to Internet
policy-map type inspect trusted2guest_policy
 class type inspect inspect_protocols
  inspect
 class class-default
  drop
! This policy permits only essential traffic (VPN/management etc.)
! to the router. Everything else is blocked from entering the router.
policy-map type inspect net2self_policy
 class type inspect edge_fw
  pass
 class class-default
  drop
! Traffic originating from the router towards internet is allowed.
! First ones matches the outbound VPN and other essential traffic.
! Second class matches the management traffic. Everything else
! is dropped.
policy-map type inspect self2net_policy
 class type inspect outbound_traffic
  pass
 class type inspect mgmt_traffic
  pass
 class class-default
  drop
!
! Security zone definitions
!
zone security corpnet
 description Corporate net
zone security internet
 description ISP network.
zone security trustednet
 description Home VPN network
zone security guestnet
 description Home Guest network
```

```
!
! Zone pairs and policies between them
!
zone-pair security trusted2internet source trustednet destination internet
 description Traffic from trusted network to Internet
 service-policy type inspect trusted2net_policy
zone-pair security trusted2corp source trustednet destination corpnet
 description traffic from trusted network to corporate
 service-policy type inspect pass_all_policy
zone-pair security trusted2guest source trustednet destination guestnet
 description traffic from trusted network to guest
 service-policy type inspect trusted2guest_policy
zone-pair security internet2self source internet destination self
 description Traffic from Internet to Router
 service-policy type inspect net2self_policy
zone-pair security corp2trusted source corpnet destination trustednet
 description traffic from corporate to trusted home network
 service-policy type inspect pass_all_policy
! corp2guest blocked
zone-pair security guest2internet source guestnet destination internet
 description Traffic from guest to Internet
 service-policy type inspect trusted2net_policy
! guest2trusted blocked
zone-pair security self2internet source self destination internet
 service-policy type inspect self2net_policy
!
! Access Lists
ip access-list extended fw_acl
 permit esp any any
 permit udp any any eq isakmp
 permit udp any eq isakmp any
 permit udp any eq non500-isakmp any
 permit udp any any eq 848
 permit udp host <public ntp server1> eq ntp any
 permit udp host <public ntp server2> eq ntp any
 permit tcp <subnet from which ssh is allowed> any eq 22
 permit udp any any eq bootpc
 permit icmp any any
 deny   ip any any
ip access-list extended fw_mgmt_acl
 remark ---- traffic from mgmt network to the spoke
 permit ip <management subnet>  host 10.32.227.161
ip access-list extended mgmt_acl
 remark ---- traffic to management subnet
 permit ip host 10.32.227.161 <management subnet>
ip access-list extended outbound_acl
 permit esp any any
```

```
 permit udp any any eq isakmp
 permit udp any eq isakmp any
 permit udp any any eq non500-isakmp
 permit udp any eq non500-isakmp any
 permit udp any any eq ntp
 permit tcp any eq 22 any
 permit tcp any eq telnet any
 permit udp any any eq bootps
 permit icmp any any
 deny   ip any any
!
interface Tunnel13
description - DMVPN interface connecting to corporate
zone-member security corpnet
interface FastEthernet0
 description - outside interface connecting to ISP
 zone-member security internet
interface BVI1
 description - inside interface/trusted network
 zone-member security trustednet
interface BVI2
 description - guest network
 zone-member security guestnet
!
```

Table 2 lists ZFW diagnostics and sample outputs.

Table 2. ZFW Diagnostics and Sample Outputs

show zone security	Shows zones, descriptions, and interfaces zones are applied to
show zone-pair security	Shows zone pairs and service policy associated with each zone pair
show zone-pair security source <source security name> destination <destination security name>	Shows zone pair specified, description, and service policy associated with the zone pair
show policy-map type inspect zone-pair <zone-pair name>	Shows traffic matched or dropped between zone pairs, service policies, and class map used, and inspects statistics
show policy-map type inspect <policy-map name>	Shows class maps applied to policy map and actions

```
Router#show zone security
zone self
  Description: System defined zone
zone corpnet
  Description: Corp. net
  Member Interfaces:
    Tunnel10
    Tunnel11
    Tunnel12
    Tunnel13
    Tunnel14
```

```
zone internet
  Description: ISP network.
  Member Interfaces:
    FastEthernet4
zone trustednet
  Description: Home VPN network
  Member Interfaces:
    Vlan10
zone guestnet
  Description: Home Spouse&Kids network
  Member Interfaces:
    Vlan20

Router#show zone-pair security
Zone-pair name home2internet
Description: Traffic from home to Internet
    Source-Zone trustednet  Destination-Zone internet
    service-policy trustednet2net_policy
Zone-pair name trustednet2corpnet
Description: traffic from trusted net to corporation
    Source-Zone trustednet  Destination-Zone corpnet
    service-policy trustednet2corpnet_policy
Zone-pair name trustednet2guestnet
Description: traffic from home to guest
    Source-Zone trustednet  Destination-Zone guestnet
    service-policy trustednet2guest_policy
<output omitted>

Router#show zone-pair security source trustednet destination internet
Zone-pair name trustednet2internet
Description: Traffic from trustednet to Internet
    Source-Zone trustednet  Destination-Zone internet
    service-policy trustednet2net_policy

Router#show policy-map type inspect zone-pair trustednet2corpnet

policy exists on zp trustednet2corpnet
 Zone-pair: trustednet2corpnet

  Service-policy inspect : trustednet2corpnet_policy

    Class-map: phone-cmap (match-any)
      Match: protocol sip
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol skinny
        200 packets, 4736 bytes
```

```
        30 second rate 0 bps

    Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [55716:0]
        udp packets: [676:0]

        Session creations since subsystem startup or last reset 185
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [4:1:1]
        Last session created 2w2d
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        Last half-open session total 0

     Class-map: engineer-http-cmap (match-all)
       Match: user-group group-engineer
       Pass
         7000 packets, 952951 bytes

     Class-map: class-default (match-any)
       Match: any
       Drop
         5647 packets, 228182 bytes

Router#show policy-map type inspect trustednet2corpnet_policy
  Policy Map type inspect trustednet2corpnet_policy
    Class phone-cmap
      Inspect
    Class engineer-http-cmap
      Pass
    Class class-default
      Drop
```

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, IPS can also block many of the attacks.

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

The IPS signatures are periodically published on Cisco.com. These signature files need to be downloaded to the Cisco IOS Software router periodically so that the IPS signature set is up-to-date. Automatic signatures updates

are possible by using either the Cisco IOS IPS automatic update feature or a management tool that supports pushing signatures to Cisco IOS Software routers.

Note: IPS 4.0 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 5.0.

IPS 5.0 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 set up only once. A 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 the files: http://www.cisco.com/cisco/software/release.html?mdfid=281442967&catid=268438162&softwareid=280775022&release=S573-COMP&relind=AVAILABLE&rellifecycle=&reltype=latest&i=rp
- Signature file: IOS-Sxxx-CLI.pkg, where xxx is the version number; choose the latest version
- Public key file: realm-cisco.pub.key.txt at http://download-sj.cisco.com/cisco/ciscosecure/ids/sigup/5.0/ios/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 the Return key. You can use the **dir** command to check the current directory. (On some Cisco IOS Software platforms primary disk space may not be called “flash”. In that case use the appropriate 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 CVO 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 cvo/IOS-S312-CLI.pkg from <ip address>  (via Tunnel13):
!!OO!!!!!!!!!!!!!!O!!!!!!!!!!!!!
[OK–7686949 bytes]
```

- Refer to the Cisco IOS Software IPS resource page at http://www.cisco.com/go/iosips for design considerations and best practices. Getting Started with Cisco IOS IPS with 5.x Format Signatures at http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd805c4ea8.shtml 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 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.

The 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 3 gives the Cisco IOS IPS diagnostics.

Table 3. 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 enables 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 (e.g., ISP DNS servers).

Refer to the Split DNS User Guide at http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htspldns.html for more details.

Split DNS Configuration

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

```
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 4 provides Split DNS diagnostics.

Table 4. 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

Object Group-Based ACLs

Object group-based ACLs (OGACLs) are used for configuring and managing large ACLs. This feature allows you to classify users, devices, or applications into groups, so you can apply policies based on a group classification. This feature allows for separation of ownership of different components, a reduction in configuration size, and improved ACL management and readability. Because OGACLs are an abstraction of standard Cisco IOS ACLs, you can use OGACLs where most traditional ACLs are used. However, OGACLs are not currently supported in cryptography-map traffic-selector ACLs.

There are two types of object groups: network object groups and service object groups. Network object groups define a group of hosts or subnet addresses, and service object groups define a group of services such as protocols and ports.

The syntax to configure OGACLs is similar to that of standard ACLs, but you can replace addresses, ports, and protocols with object-group names that you define:

```
ip access-list extended <acl_nam>
  [permit | deny] object-group <service_obj_grp_name> object-group
<source_obj_grp> object-group <dest_obj_grp>
```

You must first configure the necessary service or network object groups.

Service object-group configuration:

```
object-group service <service_obj_group_name>
  [protocol | port]
```

Network object-group configuration:

```
 object-group network <network_name>
 [{host <host_addr> |  <net_addr> <netmask> | group-object <nested_net_og>]
```

For the network object group, configuring a network with a mask requires use of the network mask, not the wildcard mask used in traditional ACLs. OGACLs are applied to an interface the same way that traditional ACLs are.

Because network and service object groups are separated, OGACLs are easier to edit than traditional ACLs. For example, in traditional ACLs, adding a permit statement to another host requires an additional line in the ACL

configuration. With OGACLs, you can simply add the host to the appropriate network object group. The OGACL permit statements can be left as is.

Object Group-Based ACL Configuration

The following shows a sample configuration of OGACLs. The traditional ACL configuration is also included afterward for comparison.

```
! OGACL Auth-Proxy Inbound ACL
ip access-list extended auth_proxy_inbound_acl
 permit object-group auth_proxy_inbound_acl_service any any
 permit ip any object-group auth_proxy_inbound_acl_ip_host
 permit object-group auth_proxy_inbound_acl_ports any any
 deny ip any object-group auth_proxy_inbound_acl_deny_networks

object-group service auth_proxy_inbound_acl_service
 tcp eq domain
 udp eq bootps
 udp eq domain

object-group network auth_proxy_inbound_acl_ip_host
 host 10.70.168.189
 host 10.102.6.248

object-group service auth_proxy_inbound_acl_ports
 udp range 2326 2340
 udp range 5060 5061
 udp eq 5445
 udp range 24576 24656
 tcp range 1719 1720
 udp eq tftp
 tcp range 5060 5061
 tcp eq 2000
 tcp eq 2443
 udp range 16384 32767

object-group network auth_proxy_inbound_acl_deny_networks
 10.68.0.0 255.252.0.0
 10.16.0.0 255.240.0.0
 10.107.0.0 255.255.0.0

interface BVI1
 ip access-group auth_proxy_inbound_acl in

……

! Traditional Auth-Proxy Inbound ACL used for comparison
```

```
ip access-list extended auth_proxy_inbound_acl
 permit tcp any any eq domain
 permit udp any any eq bootps
 permit udp any any eq domain
 permit ip any host 10.70.168.189
 permit ip any host 10.102.6.248
 permit udp any any range 2326 2340
 permit udp any any range 5060 5061
 permit udp any any eq 5445
 permit udp any any range 24576 24656
 permit tcp any any range 1719 1720
 permit udp any any eq tftp
 permit tcp any any range 5060 5061
 permit tcp any any eq 2000
 permit tcp any any eq 2443
 permit udp any any range 16384 32767
 deny   ip any 10.68.0.0 0.3.255.255
 deny   ip any 10.16.0.0 0.15.255.255
 deny   ip any 10.107.0.0 0.0.255.255

interface BVI1
 ip access-group auth_proxy_inbound_acl in
```

Table 5 lists OGACL diagnostics and sample outputs.

Table 5. OGACL Diagnostics and Sample Outputs

show object-group	Shows all network and service groups configured
show object-group <obj_group_name>	Shows members of the object group specified
show ip access-lists	Shows all traditional and object group

```
Router#show object-group
Network object group auth_proxy_inbound_acl_hosts
 10.68.0.0 255.252.0.0
 10.16.0.0 255.240.0.0
 10.107.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
Service object group auth_proxy_inbound_acl_services
 tcp eq domain
 udp eq bootps
 udp eq domain
…
Router#show ip access-lists
Extended IP access list auth_proxy_inbound_acl
    10 permit object-group auth_proxy_inbound_acl_service any any
    20 permit ip any object-group auth_proxy_inbound_acl_ip_host (84 matches)
    30 permit object-group auth_proxy_inbound_acl_ranges_ports any any
```

```
    40 permit object-group auth_proxy_inbound_acl_tcp any object-group
auth_proxy_inbound_acl_dest
```

Router Security and Authentication

It is assumed that the router at a remote end 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 Cisco Virtual Office – Public Key Infrastructure Integration deployment guide at http://www.cisco.com/go/cvo.

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 to 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
```

Table 6 lists some important diagnostic and show commands for PKI.

Table 6. 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 that 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, 2014”

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 keywords 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 bypass 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

Note: This configuration goes on the hub router:

```
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 and 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 Cisco Virtual Office – Public Key Infrastructure Integration at http://www.cisco.com/go/cvo.

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 unusable. 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 . The user will have to contact the administrator to restore VPN connectivity.

This feature has no 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 it 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. A savvy Cisco IOS Software end user may be able to look at the router configuration using this method. This access 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 help 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 a user changes the 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 Integrated Services 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.
```

User and Device Security and Authentication

The security and authentication features in this section mainly help 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. Authentication proxy (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, users 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 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 access control entries 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 the authentication process is defined by an intercept ACL.

The authenticated sessions will 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 the user will 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 auth-proxy. 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 auth-proxy. 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 (UVA) is enabled on the IP phone.

Table 7 lists some important authentication-proxy diagnostics commands.

Table 7. Authentication-Proxy Diagnostics Commands

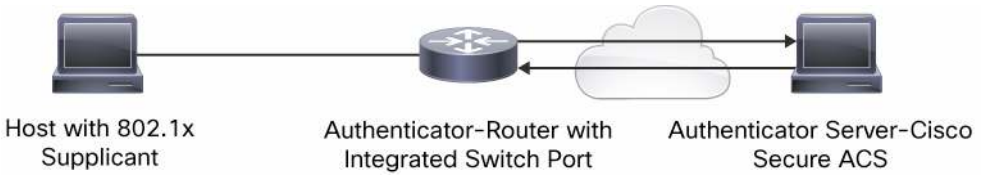
show ip auth-proxy cache	Displays the existing auth-proxy sessions
show ip auth-proxy config	Displays the current configuration
clear ip auth-proxy cache [*/<ip address>]	Clears auth-proxy sessions
debug ip auth-proxy [options]	Enables auth-proxy debugs

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 or placed on a guest VLAN with limited access.

This authentication requires an 802.1x client (called supplicant) running on the device (Figure 3). The supplicant is the 802.1x client that runs on the device that needs to be authenticated. Supplicant support may come as part of the operating system or as third-party software. Care should be taken not to run multiple supplicants at the same time. The authenticator is the CVO spoke router and the authentication server is a Cisco Secure Access Control Server (ACS) in this case.

Figure 3. 802.1x Components



Many devices such as IP phones do not have an 802.1x supplicant. In order to accommodate clientless devices, 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 aut-proxy is sufficient. Table 8 compares Authentication Proxy and 802.1x authentication.

Table 8. Authentication Proxy vs. 802.1x

	Authentication Proxy	802.1x
Protocol used	HTTP—Can be configured on any router on the	IEEE 802.1x—Should be configured on the immediate networking

	Authentication Proxy	802.1x
	network path.	device (spoke router on Cisco Virtual Office). 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). There are 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.

The authentication mechanisms for 802.1x used in Cisco Virtual Office deployment are EAP-MD5-Challenge, EAP-PEAP, and EAP-TLS (other EAP protocols also will work as long as the supplicant and the authentication server support them). The 802.1x supplicant running on the hosts establishes an EAP session with the Cisco Secure ACS and authenticates itself using username/password credentials. The user account needs to be configured on the Cisco Secure ACS. The supplicant needs to be configured to perform the EAP-MD5-Challenge, EAP-PEAP, or EAP-TLS. EAP-PEAP and EAP_TLS can be optionally configured to authenticate the Cisco Secure ACS using digital certificates. In this case the ACS should be preloaded with a certificate issued by a Certificate Server. EAP-TLS authenticates the end host using digital certificates. So each host should have its own certificate from a Certificate Server that is trusted by the ACS server.

The configuration interface of the supplicants will depend on their vendor and the supported operating system. Supplicants may provide different options to gather the user credentials. It can prompt the user for credentials at the time of authentication, allow the credentials to be preconfigured, or get the credentials from the operating system (Windows login credentials, for example).

In the following configurations, VLAN 10 is the trusted VLAN and VLAN 20 is the guest VLAN. Each switch port is individually configured to enable 802.1x authentication. It is possible to configure some ports with authentication enabled and some without authentication.

Basic Port Authentication

This mode is the basic mode of operation of this feature. When the port authentication is enabled, the router asks for credentials before the host can establish network access. If the connected host has an 802.1x supplicant installed, it will respond with the credentials. If the validation is successful, the port will be enabled and be part of the designated VLAN. If the authentication fails, the port is shut down.

Note: Note: Dynamic VLAN assignment can also be configured on the ACS.

Sample configuration:

```
aaa new-model
aaa group server radius dot1x
 server-private <ip address> auth-port 1812 acct-port 1813 key 0 <key>
aaa authentication dot1x default group dot1x
```

```
! Enable dot1x feature globally
dot1x system-auth-control
!
interface FastEthernet2
 switchport access vlan 10
 ! Enable authenticator functionality
 dot1x pae authenticator
 ! Enable dot1x on this interface
 dot1x port-control auto
 ! Enable periodic re-authentication
 dot1x reauthentication
 ! Re-authentication timeout.
 dot1x timeout reauth-period  120
!
```

The configuration needs to be added to each switch port that needs to do dot1x authentication.

Guest and Auth-Fail VLAN

Hosts that do not have 802.1x supplicant capability will not be able to respond to the EAPoL requests initiated by the router. Normally the port will be shut down if the router identifies that the connected host is clientless. If the guest VLAN feature is enabled, the port will be associated with a different VLAN instead of shutting down. Similarly, if a host with an 802.1x supplicant fails the authentication, the auth-fail VLAN feature can be used to associate it with a different VLAN instead of providing no access. In the following configuration, both the guest and auth-fail VLANs are configured to be VLAN 20.

```
interface FastEthernet2
 switchport access vlan 10
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 20
 dot1x auth-fail vlan 20
!
```

Single-Host or Multihost Mode

The port can be configured to allow only one host or multiple hosts connecting to it. In single-host mode, only one host will be allowed to connect to the port. In multihost mode, more than one host can be connected to the port using an Ethernet hub attached to it. A single host directly connected to the port also will work in multihost mode. Single-host mode is enabled by default. It should be noted that in multihost mode, the authentication status of the connected port is determined by the first host that does the authentication process. If the first host is authenticated, then rest of the hosts also get the same access. If the authentication fails for the first host, then the remaining hosts also get the same limited access. It is recommended to use single-host mode. It is more secure to allow only one authorized host per port than to share one authorized port with potentially unauthorized hosts.

```
interface FastEthernet2
 dot1x host-mode single-host
 ! “dot1x host-mode multi-host” is the other option
```

Forced Authorization and Unauthorization

By enabling forced authorization on a port, the clientless hosts can connect to it and still be part of the trusted VLAN. This connection has the same effect as not enabling dot1x on the port. It can be particularly useful if a user wants to connect an IP phone or other device that does not have a supplicant but still needs to be part of the secure VLAN. Any host can be connected to this port and be part of the secure VLAN without going through 802.1x authentication. Similarly, the port can be forced to be unauthorized. This process has the same effect as shutting down the port.

```
interface FastEthernet2
 dot1x port-control force-authorized
 ! “dot1x port-control force-unauthorized” has the opposite effect
```

Reauthentication

The port can be configured to reauthenticate the hosts periodically. The reauthentication period is also configurable. Periodic reauthentication will remove the hosts from the trusted VLAN if its credentials are removed from the RADIUS server. It may not be helpful to detect if a new user is using the authenticated host, mainly because most of the supplicants cache the credentials after they are entered by the original user. If the Ethernet cable is moved to a new host or the host is rebooted, the switch port will detect Layer 2 termination and clear the associated 802.1x session. Clearing associated sessions may not be possible if the port is expanded using a hub. A bad user can then spoof the MAC address of the authenticated host on a different host, and try to use the existing 802.1x session. If reauthentication is enabled, the spoofed host can be forced to perform authentication when the reauthentication timer fires.

```
interface FastEthernet2
 switchport access vlan 10
 dot1x pae authenticator
 dot1x port-control auto
 dot1x timeout reauth-period 600
 dot1x reauthentication
!
```

The timeout can also be initiated by the RADIUS server. The **aaa authorization network default group dot1x** command gives authority to the network group called dot1x.The timeout period is defined on the RADIUS server itself.

```
aaa authorization network default group dot1x
interface FastEthernet2
 switchport access vlan 10
 dot1x pae authenticator
 dot1x port-control auto
 dot1x timeout reauth-period server
 dot1x reauthentication
!
```

On the ACS, the time feature is located under Interface Configurations -> RADIUS (IETF) -> select [027] Session Time Out. Depending on which column was selected, session timeout will appear under group settings or user settings and enter a value (in seconds).

Voice VLAN

Using this feature, Cisco IP phones can be placed in a separate VLAN when they are connected to an Ethernet switch port. This feature is not an 802.1x feature, but it is useful because the IP phones may not support an 802.1x supplicant. IP phones can be placed in a separate VLAN bypassing 802.1x authentication. That VLAN can be configured to provide only voice access. The voice VLAN can also use the same DHCP pool as the trusted VLAN by using the **ip unnumbered sub-interface** command. If an IP phone is a third-party IP phone, the voice VLAN feature will not work automatically. Using MAC bypass will permit a third-party phone to be placed onto the voice VLAN.

```
interface FastEthernet2
 switchport access vlan 10
 switchport voice vlan 11
 dot1x pae authenticator
 dot1x port-control auto
```

MAC Authentication Bypass

In the scenario where the device attaching to the Cisco Virtual Office spoke does not have an 802.1x client, the ISR G2 transparently detects the absence of a client and automatically switches to MAC Authentication Bypass (MAB) as an alternative method to authenticate the device. MAB consists of validating the MAC address of the connecting device against a list of trusted MAC addresses on the AAA server. As in the case of 802.1x, the result of this authentication determines which VLAN the device will be placed on, and thus which resources it will have access to: if the MAC address was valid, it will be placed on the trusted (corporate) VLAN; otherwise, it goes on the guest VLAN.

Note: There are multiple 802.1x timeouts available that can be configured, depending on the requirements. These timers are essential, especially for MAB-enabled ports, where 802.1x has to timeout before execution of MAB can begin. To reduce the default timeout, two timers are modified, tx-period and quiet period. The tx-period is the number of seconds the router waits for a response from the device. It plays an important role in determining whether or not an 802.1x client exists on the device. The quiet period specifies the time that the router would wait before trying again after a failed authentication. For optimal performance, it is recommended that you configure these timers depending on your deployment.

interface FastEthernet2

```
switchport access vlan 10
switchport voice vlan 11
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 5
dot1x timeout tx-period 3
dot1x auth-fail vlan 20
dot1x auth-fail max-attempts 1
dot1x guest-vlan 20
```

802.1x Diagnostic Commands

Table 9 lists the 802.1x diagnostic commands.

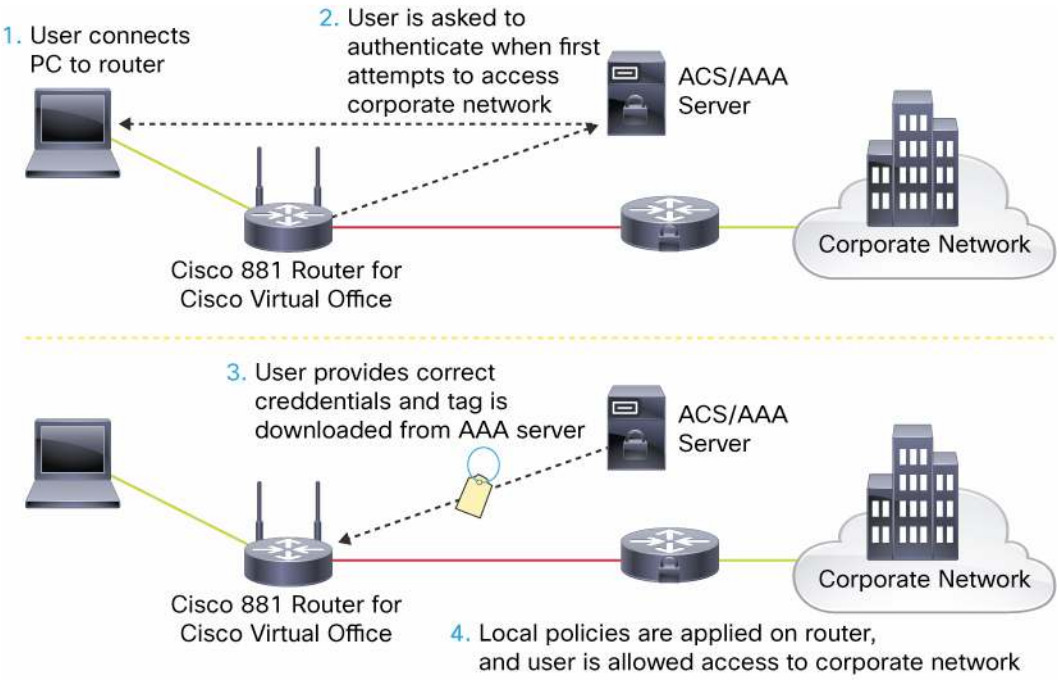
Table 9. 802.1x Diagnostic Commands

Command	Description
show dot1x	Display 802.1x overview.
show dot1x interface [FastEthernet | Vlan] [interface number]	Display 802.1x status for the specified interface.
show dot1x interface [Fast Ethernet | Vlan] [interface number] detail	Display detailed 802.1x status for the specified interface, including the details about the associated clients.
clear dot1x all	Clear all the 802.1x associations.
clear dot1x interface [FastEthernet | Vlan] [interface number]	Clear all the 802.1x associations on a specified interface.
dot1x re-authenticate	Force reauthentication of all existing clients.
dot1x re-authenticate interface [FastEthernet | Vlan] [interface number]	Force reauthentication of clients associated to a specified interface.
debug dot1x all	Enable all 802.1x debugs.

User Group Firewall

User Group Firewall is a mechanism to authenticate each user and provide access privileges based on the type of user being authenticated. The authentication is done by a RADIUS server. The user initially has limited or no access to the protected network. When the user is authenticated, access privileges are established for the IP address from which the user is accessing the network. The access privileges depend on which user group the user belongs to on the RADIUS server. (Refer to Figure 4 for the work flow.)

Figure 4. UGFW Work Flow



The authentication process begins when you make an HTTP request to the protected network. If the IP address of that device is not already authenticated, the HTTP request is intercepted by the router and replaced with a webpage querying for username and password. You must enter the assigned username and password. The credentials are then forwarded to a RADIUS server for validation.

After you are authenticated by the RADIUS server, a user tag is downloaded from the server. The tag is configured in the group you belong to on the RADIUS server. The router then installs the corresponding access policy that matches the downloaded tag. An access policy must be defined on the router for each possible tag.

This local policy configuration allows flexibility so that users in different locations may have different access controls for the same tag. (For example, a user accessing from a remote-access node may be given less access compared to the same user authenticating from an enterprise location.) An end host can also be part of multiple user groups, so different tags can be downloaded, providing various levels of access.

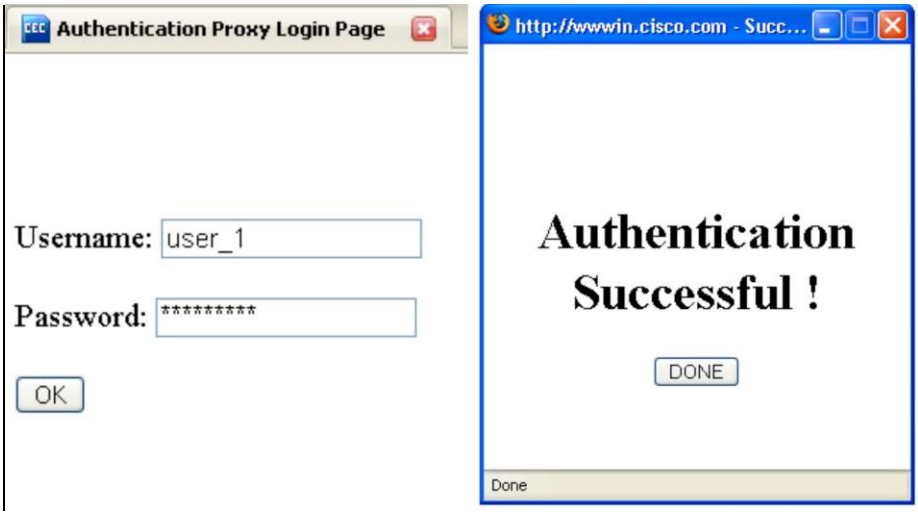
You need to configure an intercept access control list (ACL) as part of the UGFW configuration. This ACL defines what traffic needs to be authenticated. The UGFW feature works only with Zone-Based Policy Firewall. The user tags are configured as traffic classification rules.

On the client side, you are prompted to authenticate by entering a username and password combination (refer to Figure 5). (Your user credentials must first be added to the authentication, authorization, and accounting [AAA] server.)

Note: This procedure is similar to Cisco Authentication Proxy except that a tag is downloaded from the server. From the user side, authentication steps are the same as those for authentication proxy. The user setup in the AAA server is also configured similarly. Please refer to http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/scdauthp.html for a more detailed explanation of authentication proxy.)

After a user is authenticated, traffic from that user will start matching the tag and will follow the traffic rules configured for it. When the end user is associated with the user group, inspection is enabled for all traffic and protocols coming from that source.

Figure 5. Authentication Prompt and Success Screen After a User Successfully Authenticates. Clicking “Done” After Successful Authentication Allows Access to the Corporate Network.



Server-Side Configuration

A tag that associates a user to a user group must first be configured on an AAA server. The tag name is specified as a vendor-specific Attribute-Value (AV) pair. This guide uses Cisco Secure Access Control Server (ACS) v5.2. In this version of Cisco Secure ACS, the AV pair is configured under Policy Elements → Authentication Profiles. Please refer to the Cisco Secure Access Control Server Deployment guide at http://www.cisco.com/go/cvo for more detailed ACS configuration and deployment documentation.

In this case, the Cisco AV pairs are specified in the format **tag-name**=<name of tag> followed by the privilege level for the tag: **priv-lvl**=<privilege level>. This tag must match the tag configured locally on the router for successful authentication. If the tag matches, the user will be associated with that user group.

Spoke Router Configuration

On the Cisco Virtual Office setup, the zone pairs to which UGFWs are applied are the trustednet-to-corpnet zone pair. (Refer to Figure 2 for a zone-pair diagram). In this zone pair, when the user's PC downloads the tag from the AAA and is associated with a user group, all traffic is allowed from trustednet to corpnet. If authentication fails, then traffic is dropped from the trustednet to the corpnet. Return traffic from corpnet to trustednet is allowed to pass by default.

User Group Firewall Sample Configuration

Following is the configuration for User Group Firewall on the Cisco Virtual Office spoke router.

On the spoke router, apply the following:

```
! Enable ip http server to allow access to the RADIUS server
ip http server

! Configure AAA parameters.  This AAA should also have the user group tag
configured on it.

aaa group server radius authproxy
 server-private <server ip addr> auth-port 1812 acct-port 1813 key 7 <key>
 ip radius source-interface Vlan10
aaa authentication login default local group authproxy
aaa authorization auth-proxy default group authproxy

! Specify which tag to match.  Tag must match the one configured on AAA. In this
case, the tag name is 'engineer' so 'engineer' is also configured as the tag name
on the AAA server.

class-map type control tag match-all engineer-class
 match tag engineer

! Configure policy attributes for the user group.  The user group in this case is
called 'group-engineer.'  Once the user authenticates, he/she will be considered
part of the user group 'group-engineer.'

   identity policy engineer-policy
 user-group group-engineer
```

```
! Tie the tag name with the policy it should be associated with.  Here, the tag
‘engineer’ defined in ‘engineer-class’ will be associated with user group named
‘group-engineer.’  Policies for ‘group-engineer’ will be applied once the tag is
downloaded.

policy-map type control tag ugfw-tag-policy
 class type control tag engineer-class
  identity policy engineer-policy



! Specify interesting traffic to match on.  In this case, it is based on
membership of source ip address in the user-group

class-map type inspect match-all engineer-http-cmap
 match user-group group-engineer

! Define zones that must require user authentication before access

zone security trustednet
 description zone where the IP devices at home are connected which needs to have
corporate access
zone security corpnet
 description zone connecting to corporate network, tunnel interface on CVO

! Policy map to inspect traffic between trustednet and corpnet zones

policy-map type inspect trustednet2corpnet_policy
 class type inspect engineer-http-cmap
  pass
class class-default
  drop

!Configure zone-pair and apply the policy-map

zone-pair security trustednet2corpnet source trustednet destination corpnet
 description traffic from trustednet to corpnet
 service-policy type inspect trustednet2corpnet_policy

! Configure the intercept ACL

ip access-list extended auth_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
 …
```

```
!
! Map the tag-name to a template on the spoke router and associate it with an
authentication method.  auth_proxy_acl is the intercept ACL.

ip admission name auth-http proxy http inactivity-time 60 list auth_proxy_acl
service-policy type tag ugfw-tag-policy

! Apply ip admission rule to the source zone member interface

interface Vlan10
 ip admission auth-http
```

Note: Matches on user groups allow traffic of all protocol types. If further restriction is desired, add additional matches but make sure the class map is inspecting on a “match-all” criterion. For example, if only TCP traffic is allowed, the configuration should be:

```
class-map type inspect match-all engineer-http-cmap
 match user-group group-engineer
 match protocol tcp
```

Note: Configuring the following does not restrict traffic to just TCP traffic because the user group matches on all protocol types:

```
class-map type inspect match-any engineer-http-cmap
 match user-group group-engineer
 match protocol tcp
```

IP Phone Bypassing

IP phones must be bypassed because they cannot be authenticated with authentication proxy.

One method to bypass IP phones is to create a separate VLAN for the voice traffic. Creating a voice VLAN also allows you to apply different policies specifically for the IP phones that are separate from the policies for allowing the user’s PC to access the corporate network.

```
! Configure auth-proxy exemption for Cisco IP phone
identity profile auth-proxy
 device authorize type cisco ip phone policy ip-phone
identity policy ip-phone
 user-group cisco-phone

! Define policy attributes to be enforced for the IP phone
identity policy ip-phone
 user-group cisco-phone

! Define the match criteria for phone traffic.
class-map type inspect match-any ip-phone
 match protocol sip
```

```
 match protocol skinny
 match protocol dns
 match protocol https
 match protocol http

! Define policy to inspect traffic coming from the ip phone to the corpnet
policy-map type inspect ip_phone_policy
 class type inspect ip-phone
  inspect
 class class-default
  drop

! Define security zone for the ip phone
zone security ipphone
 description ipphone

! Configure a separate vlan for the IP phone and apply the proper zone to the
vlan
interface Vlan30
 description voice vlan
 ip unnumbered Vlan10
 zone-member security ipphone
 no autostate

! Configure voice vlan on interface(s)
interface FastEthernet1
 switchport voice vlan 30

! Configure zone-pair and apply the policy-map for traffic between the ip phone
and corpnet
zone-pair security ipphone-corpnet source ipphone destination corpnet
 service-policy type inspect ip_phone_policy
zone-pair security corpnet-ipphone source corpnet destination ipphone
 service-policy type inspect ip_phone_policy

! Add ip admission for the phone.  This will match the user group cisco-phone as
configured above.
ip admission name ip-phone proxy http inactivity-time 60
```

Note: After applying the configuration, you may have to reset the phone and wait a few minutes before the phone registers with the Cisco Unified Communications Manager and comes up again.

An alternative method is to create a class map to allow the protocols needed to establish the voice communication sessions to pass and add it to the policy for allowing traffic from the trustednet to the corpnet. The voice traffic policy must be defined and matched first (before other traffic) in this case.

```
! Configure auth-proxy exemption for Cisco IP phone
identity profile auth-proxy
```

```
 device authorize type cisco ip phone policy ip-phone
identity policy ip-phone
 user-group cisco-phone

! Define policy attributes to be enforced for the IP phone
identity policy ip-phone
 user-group cisco-phone

! Define the match criteria for phone traffic.  Here it is sip and skinny.
class-map type inspect match-any phone-cmap
 match protocol sip
 match protocol skinny

! Define the policy to inspect traffic between trustednet and corpnet. Make sure
to inspect the phone traffic first.
policy-map type inspect trustednet2corpnet_policy
 class type inspect phone-cmap
  inspect
 class type inspect engineer-http-cmap
  pass
 class class-default
  drop

! Define policy to inspect traffic coming back from the corpnet to the trustednet
policy-map type inspect corp2trustednet_policy
 class type inspect phone-cmap
  inspect
 class class-default
  pass

!Configure zone-pair and apply the policy-map
zone-pair security trustednet2corpnet source trustednet destination corpnet
  service-policy type inspect trustednet2corpnet_policy
zone-pair security corpnet2trustednet source corpnet destination trustednet
  service-policy type inspect corpnet2trustednet_policy

! Add ip admission for the phone.  This will match the user group cisco-phone as
configured above.
ip admission name ip-phone proxy http inactivity-time 60
```

Table 10 lists UGFW diagnostics and sample outputs.

Table 10. UGFW Diagnostics and Sample Outputs

show user-group	Shows user groups and IP address of device associated with each user group
show user-group count	Shows number of user groups and number of members in each group
show epm session ip <ip address>	Shows tag downloaded by each device (determined by IP address) and the policy applied to the device

```
Router#show user-group
```

```
Usergroup : cisco-phone
------------------------------------------------------------------------
User Name       Type     Interface              Learn         Age (min)
------------------------------------------------------------------------
10.32.229.156   IPv4     Vlan10                   Dynamic         0

Usergroup : group-engineer
------------------------------------------------------------------------
User Name       Type     Interface              Learn         Age (min)
------------------------------------------------------------------------
10.32.229.154   IPv4     Vlan10                   Dynamic         0


Router#show user-group count
Total Usergroup : 2
-----------------------------------------------------------
User Group                                  Members
-----------------------------------------------------------
cisco-phone                                   1
group-engineer                                1

Router#show epm session ip 10.32.229.156
Admission feature       : Authproxy
Identity Policy         : ip-phone

Router#show epm session ip 10.32.229.154
Admission feature       : Authproxy
Tag Received            : engineer
Policy map used         : ugfw-tag-policy
Class map matched       : engineer-class
```

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
```

References

- Cisco Virtual Office page: http://www.cisco.com/go/cvo
- Cisco IOS Software DMVPN: http://www.cisco.com/go/dmvpn
- Cisco IOS Software IPsec: http://www.cisco.com/go/ipsec

- Authentication Proxy Authentication Outbound - No Cisco IOS Firewall or NAT configuration: http://www/en/US/partner/products/sw/secursw/ps1018/products_configuration_example09186a00800942fd.shtml
- Implementing authentication proxy: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0.shtml
- Zone-Based Policy Firewall design and application guide: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml
- Cisco IOS Firewall resource page: http://www.cisco.com/go/firewall
- Cisco IOS Software IPS resource page: http://www.cisco.com/go/iosips
- IPS 5.0 signature format support and usability enhancements: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ips_v5.html
- Getting started with Cisco IOS IPS with 5.0 format signatures http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd805c4ea8.shtml
- Cisco IOS Software infrastructure security: http://www.cisco.com/go/infrastructure
- Cisco integrated services routers: http://www.cisco.com/go/isr
- Split DNS user guide: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htspldns.html
- Cisco Secure ACS user guide: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/introd.html
- User Based Firewall support guide: http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_user_fw_supp.html

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 C07-684609-01 04/12