

Cisco Virtual Office: Advanced Layered Security

Deployment Guide



This deployment guide provides detailed design and implementation information for deployment of Advanced 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 VPN deployment solution, please refer to the Cisco Virtual Office Deployment Guide at http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns430/ns855/deployment_guide_c22-493157.html.

Following are the major features included in this guide:

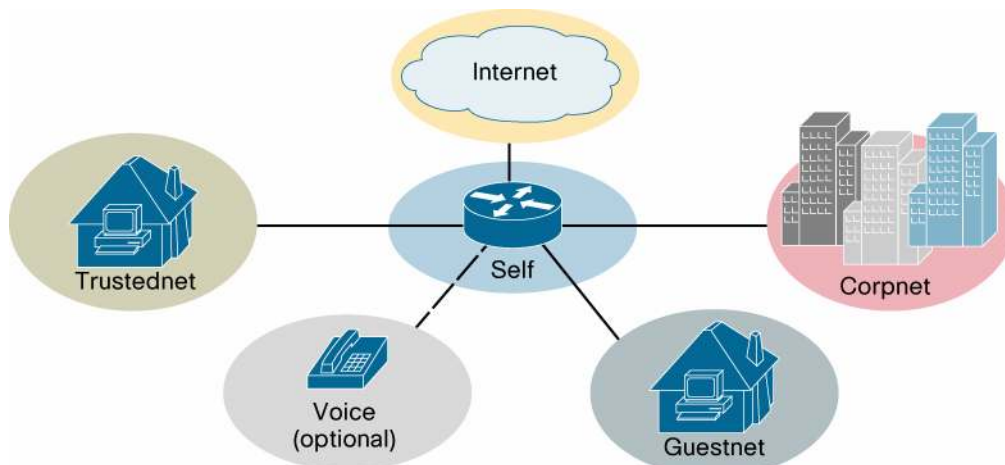
- Zone-Based Policy Firewall (ZFW)
- User Group Firewall (UGFW)
- Object Group Access Control List (OGACL)

Zone-Based Policy Firewall

Zone-Based Policy Firewall (ZFW) is a new 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.

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 1).

Figure 1. 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” (Reference 3).

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

- Corpnet: Zone connecting to corporate network, tunnel interface on Cisco Virtual Office
- 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

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. So if the router needs to be made accessible from any other zones, you must define a policy between that 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: Allow only restricted traffic (such as VPN, management network, etc.); 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 assume the default policy of not allowing any traffic between them.

Some ZFW Design Considerations

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 policies 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 where both interfaces belong to instead of self-zone policy. 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” (Reference 3).

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 Tunnell3
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 1 lists ZFW diagnostics and sample outputs.

Table 1. 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

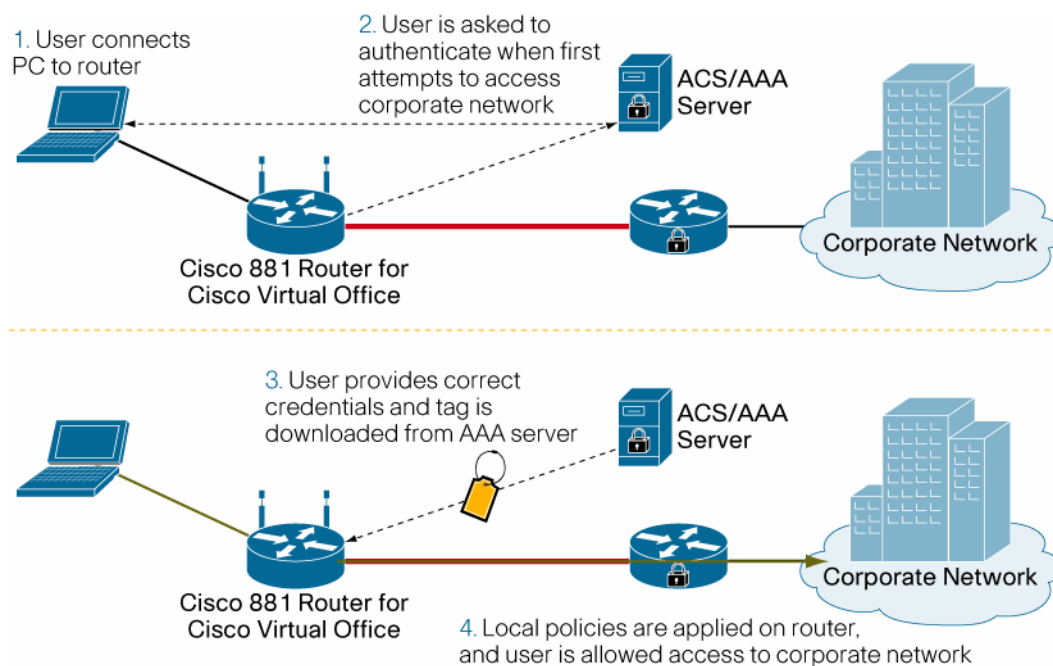
Class-map: class-default (match-any)
Match: any
Drop
5647 packets, 228182 bytes

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
```

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 2 for the work flow.)

Figure 2. 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 on a RADIUS server, which corresponds to the group you belong to. 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 that different tags can be downloaded, providing various levels of access.

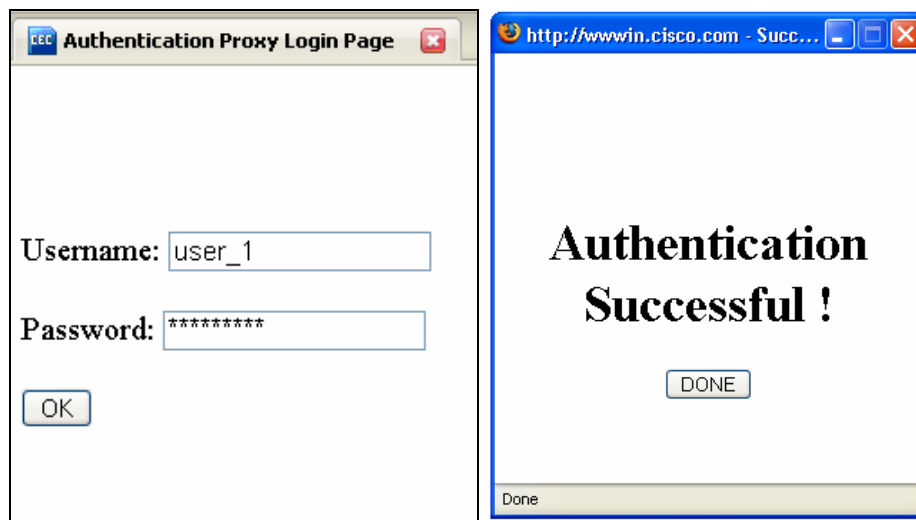
You need to configure an intercept access control list (ACL) as part of the UGFW configuration. This ACL defines what traffic needs to be authenticated. The UGFW feature works only with Zone-Based Policy Firewall. The user tags are configured as traffic classification rules.

On the client side, you are prompted to authenticate by entering a username and password combination (refer to Figure 3). (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 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 3. Authentication Prompt and Success Screen After a User Successfully Authenticates. Clicking “Done” After Successful Authentication Allows Access to the Corporate Network.



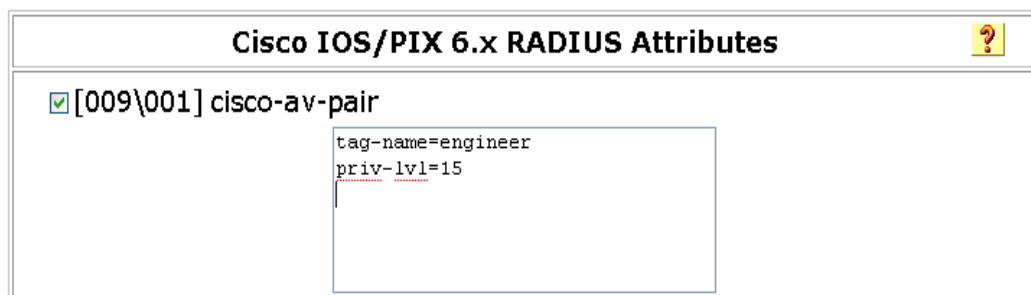
Server-Side Configuration

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. Cisco Virtual Office uses Cisco Secure Access Control Server (ACS) v4.1. In this version of Cisco Secure ACS, the AV pair is configured under the Cisco IOS® Software or Cisco PIX® 6.0 RADIUS Attributes section after the group has been created on the server. Please refer to the Cisco Secure Access Control Server Deployment guide for Cisco Virtual Office for more detailed ACS configuration and deployment documentation

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/deployment_guide_c07_458687_ns855_Networking_Solutions_White_Paper.html.

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>. Figure 4 shows a screenshot of the Cisco ACS page where the AV pairs are configured. 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.

Figure 4. Cisco Secure ACS Configuration for UGFW



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 1 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, 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 2 lists UGFW diagnostics and sample outputs.

Table 2. 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

```

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_name>
```

```
[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 BV11
 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 BV11
 ip access-group auth_proxy_inbound_acl in

```

Table 3 lists OGACL diagnostics and sample outputs.

Table 3. 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

<code>show ip access-lists</code>	Shows all traditional and object group-based ACLs and matches
-----------------------------------	---------------------------------------------------------------

```
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
```

References

- Cisco Virtual Office Deployment Guide:
http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns430/ns855/deployment_guide_c22-493157.html
- Zone-Based Policy Firewall Design and Application Guide:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml
- Cisco Secure ACS Deployment for Cisco Virtual Office:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/deployment_guide_c07_458687_ns855_Networking_Solutions_White_Paper.html
- Authentication Proxy Authentication Outbound-No Cisco IOS Firewall or NAT Configuration:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps1018/products_configuration_example09186a00800942fd.shtml
- Implementing Authentication Proxy:
http://www.cisco.com/warp/public/793/ios_fw/auth_intro.html
- Cisco Secure ACS User Guide:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/Preface.html
- Cisco Secure ACS Installation Guide:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080184928.html
- User Based Firewall Support Guide:
http://www.cisco.com/en/US/docs/ios/security/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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)