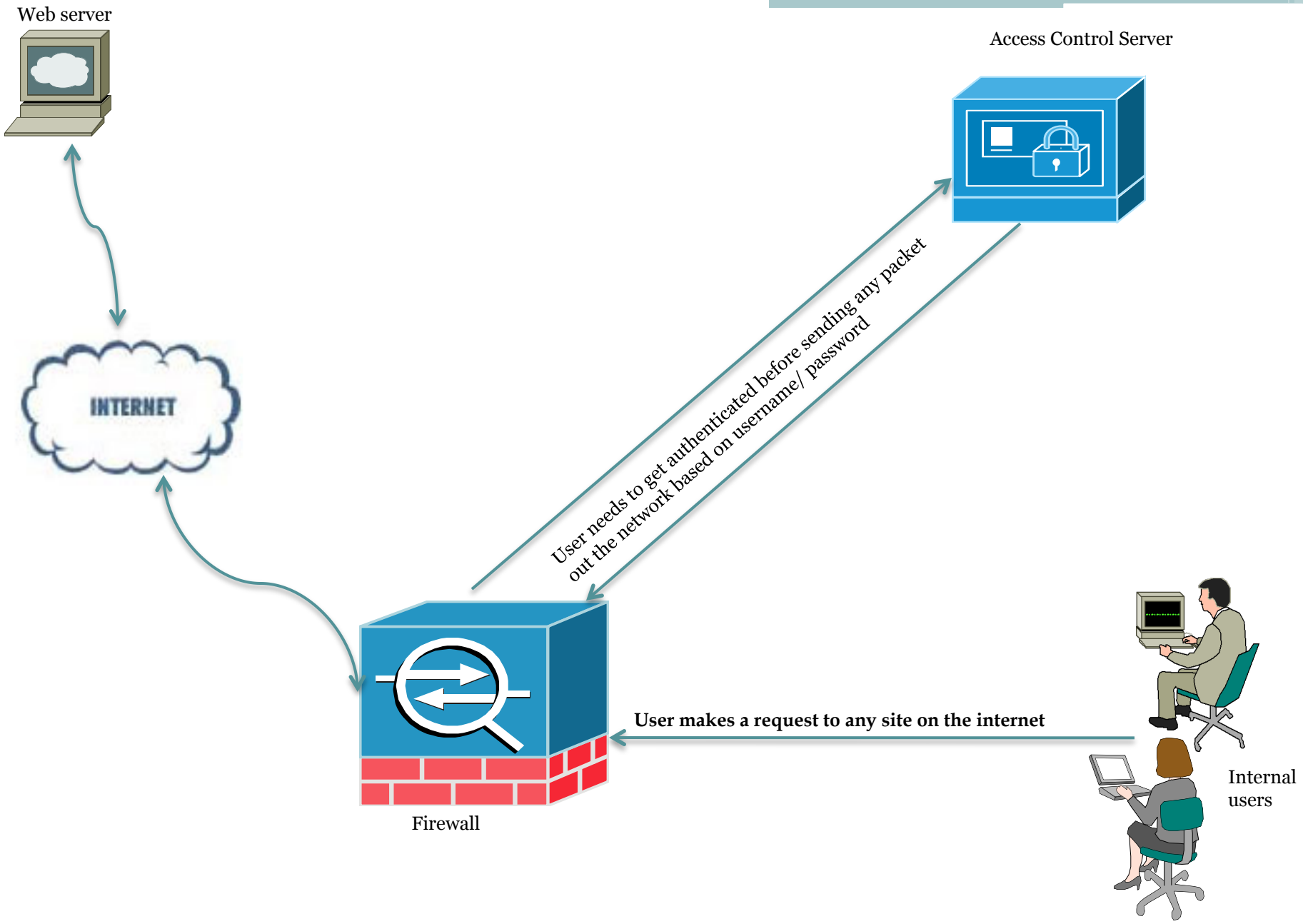
Introduction to Cut-Through Proxy

Inside to Outside

You can use access lists to control traffic based on the IP address and protocol. However, you must use authentication and authorization in order to control access and use for specific users or groups.

Authentication, which is the process of identifying users, is supported by the PIX/ASA Firewall for RADIUS and TACACS+ servers. Authorization identifies the specific permissions for a given user.

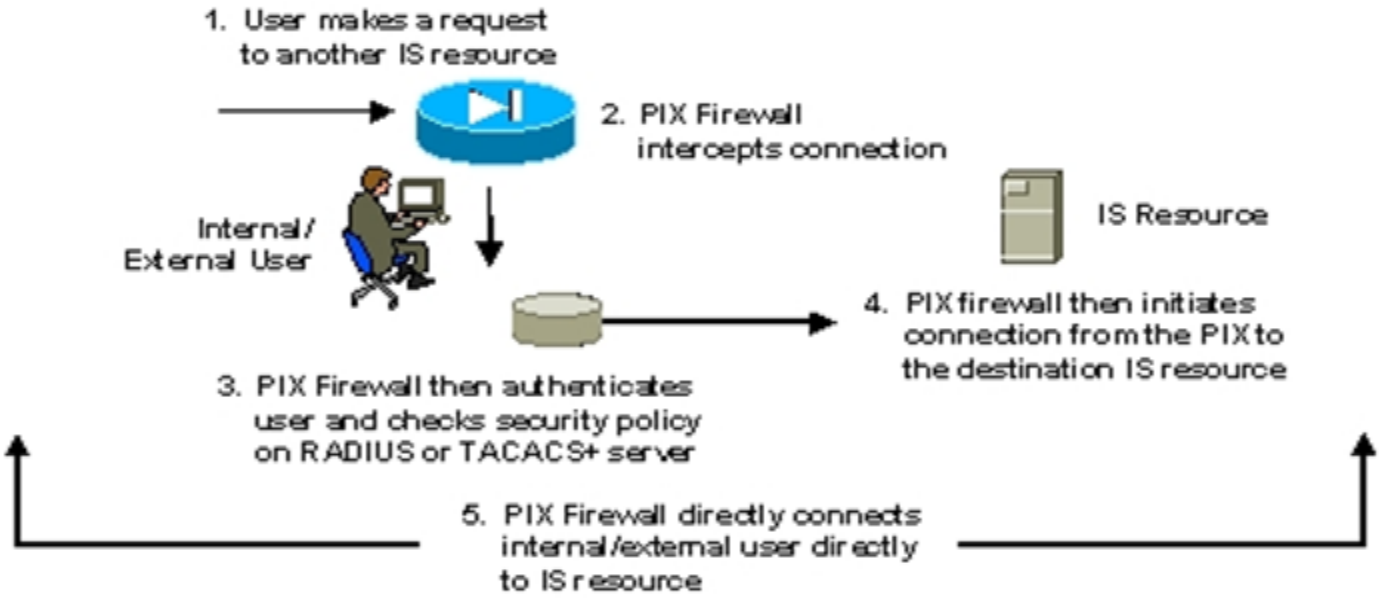

Web server
Access Control Server
INTERNET
User needs to get authenticated before sending any packet out the network based on username/ password
User makes a request to any site on the internet
Firewall
Internal users

Outside to Inside

If you want to apply authentication and authorization when an internal (local) host initiates a connection to an external (lower security) network, you need to enable it on the internal (higher security) interface.

In order to set up authentication and authorization to occur when an external host initiates a connection to an internal host, you need to enable it on the outside interface.

Authentication with Cut-Through Proxy



- **This one-time authentication at the application layer (OSI Layer 7) happens once—then the connection is passed back to the PIX Firewall's high-performance ASA engine, while maintaining session state**

Instance

AAA provides an extra level of protection and control for user access than using Access Control Lists (ACLs) alone. For example, you can create an ACL that allows all outside users to access Telnet on a server on the DMZ network. If you want only some users to access the server and you might not always know IP addresses of these users, you can enable AAA to allow only authenticated and/or authorized users to make it through the security appliance. The Telnet server also enforces authentication. The security appliance prevents unauthorized users from an attempt to access the server.

You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

Why we need Cut-through proxy

The security appliance uses "cut-through proxy" to significantly improve performance compared to a traditional proxy server. The performance of a traditional proxy server suffers because it analyzes every packet at the application layer of the OSI model. The security appliance cut-through proxy challenges a user initially at the application layer and then authenticates against standard AAA servers or the local database. After the security appliance authenticates the user, it shifts the session flow, and all traffic flows directly and quickly between the source and destination while maintaining session state information.

The authentication ports that the security appliance supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

Control User traffic/Access through firewall

- Identify users before providing services
- Once user is identified provide the right access
- Authentication and authorization for both inbound and outbound connections.
- Authentication done through telnet, ftp or http.
- Cut-through proxy for performance

Steps in order to enable authentication for Inbound and Outbound authentication

- For inbound connection, create the static and access-list command statements required to permit outside hosts to access servers on the inside network.
- If the internal network connects to the Internet, create a global address pool of registered IP addresses.
- Issue the nat command with the access-list command in order to specify the inside hosts that can start outbound connections.
- Issue the aaa-server command in order to identify the server that handles authentication or authorization.

Control User traffic

- Identify AAA server and specify protocol
- Authentication
- Authorization (optional)
- Accounting (optional)
- Customize messages (optional)
- Modify timeouts (Optional)
- Configure virtual http/telnet (Optional)

Identify AAA server and specify protocol

Aaa-server <tag> protocol tacacs+|radius

Identify the AAA server and protocol

Aaa-server <tag> [<(if_name)>] host <ip_address> [<key>] [timeout (seconds)]

- **Specify a AAA host**
- **Must specify a key for encryption**

Authentication

```
aaa authentication  include | exclude  <authentication-service> inbound | outbound <local_ip>
<local_mask> <foreign_ip> <foreign_mask> <group_tag>
```

Example: aaa authentication include any outbound any any AuthIn

OR

```
access-list <access_list_name> [extended] {deny | permit} protocol source_address mask
[operator port] dest_address mask [operator port]
```

Example:

Access-list In_Out extended permit tcp any any eq www
Access-list In_Out extended permit tcp any any eq https
Access-group outside in interface outside

Aaa authentication match In_Out inside AuthIn

The authen_service portion of the command represents the services that require authorization.
The if_name portion of the command represents the interface name from which users require authentication.

Authorization

Aaa authorization include | exclude <authorization-service> inbound | outbound <local_ip> <local_mask> <foreign_ip> <foreign_mask> <group_tag>

Aaa authorization include any outbound 172.16.16.16 255.255.255.255 0 0 0 0 AuthIn

Download of a per-user ACL from a RADIUS AAA server during authentication. With downloadable ACLs, you can store full ACLs on the AAA server and download them to the security appliance. An ACL is attached to the user or group profile on the AAA server. During the authentication process, after the user credentials are authenticated, the AAA server returns the ACL to the security appliance. The returned ACL is modified based on the source IP address of the authenticated user. This functionality is supported only with RADIUS.

Configuring authorization for network access:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080a9eddc.shtml

Accounting

Aaa accounting include | exclude <accounting-service> inbound | outbound <local_ip> <local_mask> <foreign_ip> <foreign_mask> <group_tag>

Aaa accounting include any outbound 172.16.16.16 255.255.255.255 0 0 0 0 AuthIn

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. If that traffic is also authenticated, the AAA server can maintain accounting information by username. User accounting tracks traffic that passes through the security appliance, enabling you to have a record of user activity, including when sessions start and stop, username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address.

Configuring Accounting for Network Access

http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/fwaaa.html#wp1043741

Sample Config

```
static (inside,outside) 192.168.10.10 172.16.171.13
access-list 80 permit tcp any host 192.168.10.10 eq telnet
access-list 80 permit tcp any host 192.168.10.10 eq www
access-group 80 in interface outside
aaa-server AuthIn protocol tacacs+
aaa-server AuthIn (inside) host 171.68.178.124 mykey timeout 5

aaa authentication include any inbound 172.16.171.13 255.255.255.255 0.0.0.0 0.0.0.0 AuthIn
aaa authorization include any inbound 172.16.171.13 255.255.255.255 0.0.0.0 0.0.0.0 AuthIn
aaa accounting include any inbound 172.16.171.13 255.255.255.255 0.0.0.0 0.0.0.0 AuthIn
```

Note: The ip addresses Picked randomly.

Customize message

```
auth-prompt [accept | reject | prompt] <string>
```

Accept: If a user authentication via Telnet is accepted, display the prompt string.

Reject: If a user authentication via Telnet is rejected, display the prompt string.

Prompt: The AAA challenge prompt string follows this keyword.

Modify Timeouts

```
timeout [uauth [hh:mm:ss] [absolute | inactivity]]
```

Inactivity timer

Idle time for authenticated user

Absolute timer

Absolute timeout for authentication validity

Time Outs

Absolute : *Requires a re-authentication after the uauth timeout expires. The absolute keyword is enabled by default. To set the uauth timer to timeout after a period of inactivity, enter the inactivity keyword instead.*

Inactivity : *Requires uauth re-authentication after the inactivity timeout expires.*

Uauth : *Specifies the duration before the authentication and authorization cache times out and the user has to re-authenticate the next connection, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). The default timer is absolute; you can set the timeout to occur after a period of inactivity by entering the inactivity keyword. The uauth duration must be shorter than the xlate duration. Set to 0 to disable caching.*

xlate : *Specifies the idle time until a translation slot is freed, between 0:1:0 and 1193:0:0. The default is 3 hours (3:0:0).*

Show uauth : *With this CLI command, you can view the authenticated end users, their IP addresses, and the matching downloaded ACL. To view the actual ACL, you can use the show access-list command.*

Show access-list : *To view the actual ACL you can use the show access-list command.*

Clear uauth : *This CLI command to delete all authorization caches for all users, which causes them to re-authenticate the next time they create a connection*

For more info, please refer command reference guide:
http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/t.html#wp1500148

Virtual http

Virtual HTTP redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the security appliance. The security appliance prompts for the AAA server username and password. After the AAA server authenticates the user, the security appliance redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

Virtual Telnet

The virtual Telnet option provides a way to authenticate users who require connections through the security appliance using services or protocols that do not support authentication. When an unauthenticated user establishes a Telnet session to the virtual IP address of the security appliance, the user is challenged for the username and password, and then authenticated with the AAA server. Then the user sees the Authentication Successful message, and the authentication credentials are cached in the security appliance for the duration of the user authentication timeout

virtual http ip_address [warn]

virtual telnet ip_address

Virtual http (Solves browser problem by redirecting connections)

Virtual telnet (Provide pre-authentication for those applications that don't support authentication.)

Some Useful Tips

- Do not set the authentication timeout duration to 0 seconds when using the virtual HTTP feature because this setting prevents HTTP connections to the real web server.

- The ip should not exist on the network

- The virtual ip must be statically translated to itself

Summary

This one-time authentication at the application layer (OSI Layer 7) happens once—then the connection is passed back to the PIX Firewall's high-performance ASA engine, while maintaining session state

Internal/External User

•User makes a request to another IS resource

•PIX Firewall intercepts connection

•PIX Firewall then authenticates user and checks security policy on RADIUS or TACACS+ server

•PIX Firewall directly connects internal/external user directly to IS resource

•PIX firewall then initiates connection from the PIX to the destination IS resource

Related Links

Configuration guide:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/fwaaa.html

Configuration example on cut-through authentication:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00807349e7.shtml#req

Adding an extended access-list
http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/acl_extended.pdf


CISCO