Cisco Systems
Networking Academy

Cisco.com

Network Security 1

Module 6 – Configure Trust and Identity at Layer 3

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Learning Objectives

Cisco.com

–6.1 Cisco IOS Firewall Authentication Proxy

–6.2 Introduction to PIX Security Appliance AAA Features

–6.3 Configure AAA on the PIX Security Appliance

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 6 – Configure Trust and Identity at Layer 3

6.1 Cisco IOS Firewall Authentication Proxy

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

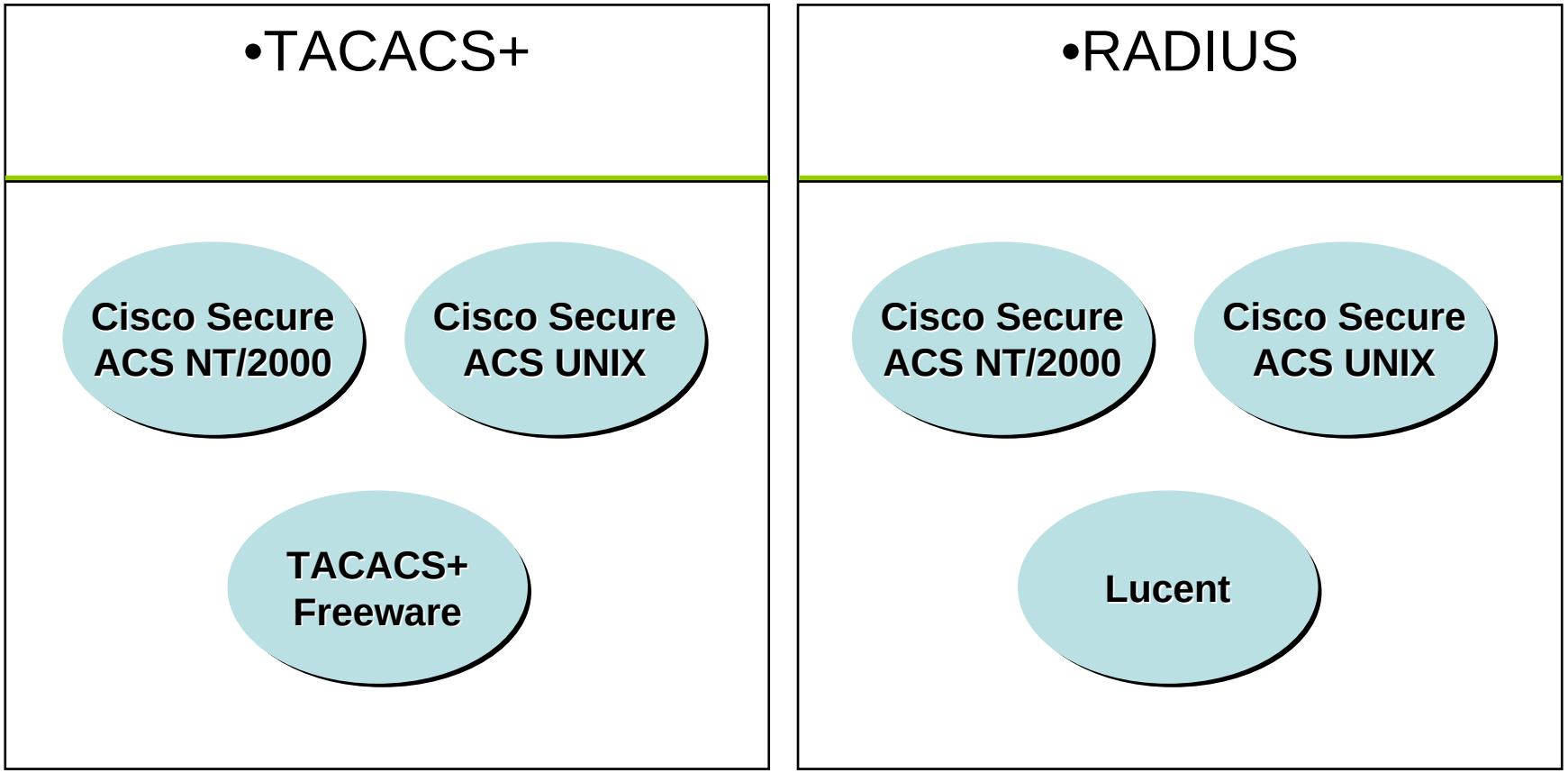
Högskolan Halmstad

What Is the Authentication Proxy?

- HTTP, HTTPS, FTP, and Telnet authentication
- Provides dynamic, per-user authentication and authorization via TACACS+ and RADIUS protocols
- Once authenticated, all types of application traffic can be authorized
- Works on any interface type for inbound or outbound traffic

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Supported AAA Servers

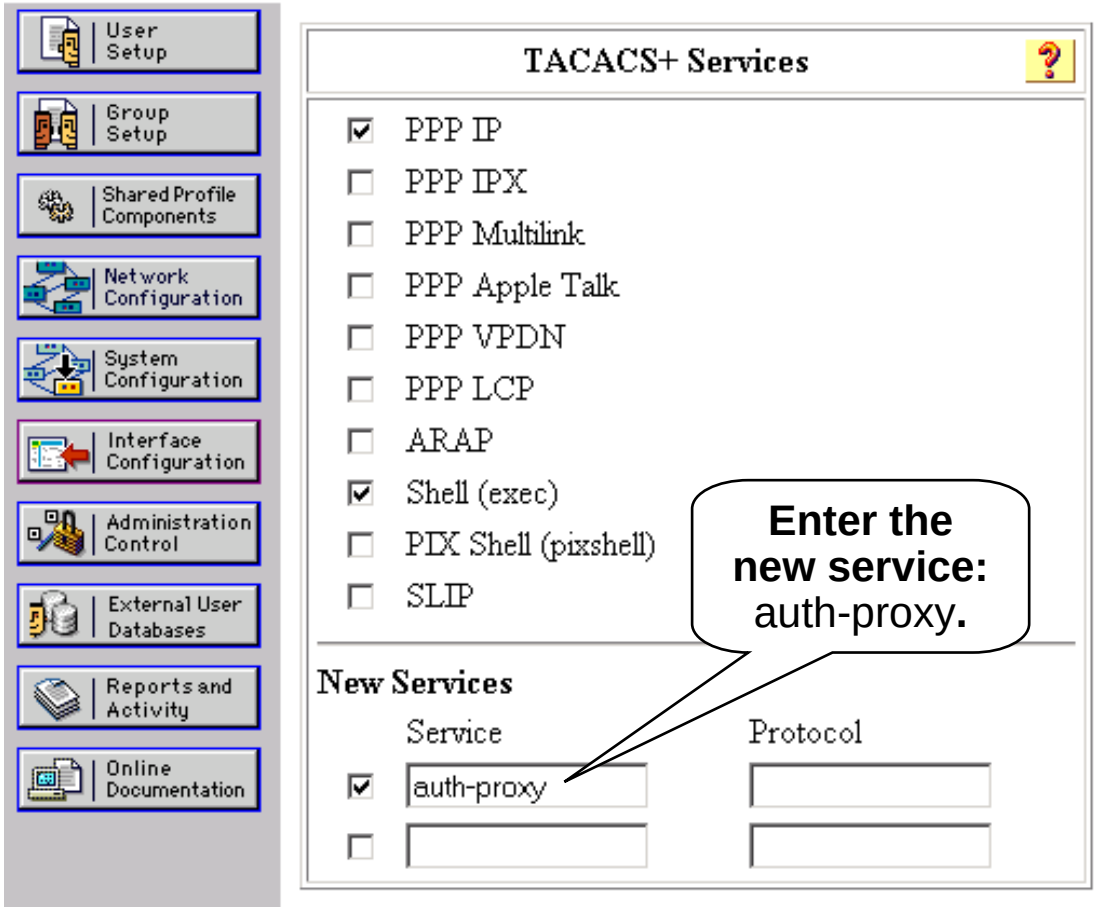


Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Create auth-proxy Service in the Cisco Secure ACS

Cisco.com

Interface Configuration



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Enable AAA

Router(config)#

```
aaa new-model
```

– Enables the AAA functionality on the router (default = disabled)

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Specify Authentication Protocols

Cisco.com

Router(config)#

```
aaa authentication login default
  method1 [method2]
```

- Defines the list of authentication methods that will be used
- Methods: TACACS+, RADIUS, or both

```
Router(config)# aaa authentication
  login default group tacacs+
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Specify Authorization Protocols

Cisco.com

Router(config)#

```
aaa authorization auth-proxy default method1
  [method2]
```

- Use the auth-proxy keyword to enable authorization proxy for AAA methods
- Methods: TACACS+, RADIUS, or both

```
Router(config)# aaa authorization auth-proxy
  default group tacacs+
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Define a TACACS+ Server and Its Key

Router(config)#

```
tacacs-server host ip_addr
```

– Specifies the TACACS+ server IP address

Router(config)#

```
tacacs-server key string
```

– Specifies the TACACS+ server key

```
Router(config)# tacacs-server host 10.0.0.3
Router(config)# tacacs-server key secretkey
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Define a RADIUS Server and Its Key

Router(config)#

```
radius-server host ip_addr
```

– Specifies the RADIUS server IP address

Router(config)#

```
radius-server key string
```

– Specifies the RADIUS server key

```
Router(config)# radius-server host 10.0.0.3
Router(config)# radius-server key secretkey
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Allow AAA Traffic to the Router


```
Router(config)# access-list 111 permit tcp host
  10.0.0.3 eq tacacs host 10.0.0.1
Router(config)# access-list 111 permit icmp any any
Router(config)# access-list 111 deny ip any any
Router(config)# interface ethernet0/0
Router(config-if)# ip access-group 111 in
```

- Create an ACL to permit TACACS+ traffic from the AAA server to the firewall
  - Source address = AAA server
  - Destination address = interface where the AAA server resides
- May want to permit ICMP
- Deny all other traffic
- Apply the ACL to the interface on the side where the AAA server resides

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Enable the Router HTTP or HTTPS Server

Router(config)#

```
ip http server
```

– Enables the HTTP server on the router

Router(config)#

```
ip http authentication aaa
```

– Sets the HTTP server authentication method to AAA

– Proxy uses HTTP server for communication with a client

Router(config)#

```
ip http secure-server
```

– Enables the HTTPS server on the router

```
Router(config)# ip http server
Router(config)# ip http authentication aaa
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Set Global Timers

Router(config)#

```
ip auth-proxy {inactivity-timer min |
 absolute-timer min}
```

- Authentication inactivity timer in minutes (default = 60 minutes)
- Absolute activity timer in minutes (default = 0 minutes)

```
Router(config)# ip auth-proxy inactivity-
 timer 120
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Define and Apply Authentication Proxy Rules

Cisco.com

Router(config)#

```
ip auth-proxy name auth-proxy-name {ftp | http
  | telnet} [inactivity-time min] [absolute-
  timer min][list {acl | acl-name}]
```

– Creates an authorization proxy rule

Router(config-if)#

```
ip auth-proxy auth-proxy-name
```

– Applies an authorization proxy rule to an interface
  - For outbound authentication, apply to inside interface
  - For inbound authentication, apply to outside interface

```
Router(config)# ip auth-proxy name aprule http
Router(config)# interface ethernet0
Router(config-if)# ip auth-proxy aprule
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Authentication Proxy Rules with ACLs

Router(config)#

```
ip auth-proxy name auth-proxy-name http list
 {acl-num | acl-name}
```

– Creates an authorization proxy rule with an access list

```
Router(config)# ip auth-proxy name aprule http
 list 10
Router(config)# access-list 10 permit 10.0.0.0
 0.0.0.255
Router(config)# interface ethernet0
Router(config-if)# ip auth-proxy aprule
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 6 – Configure Trust and Identity at Layer 3

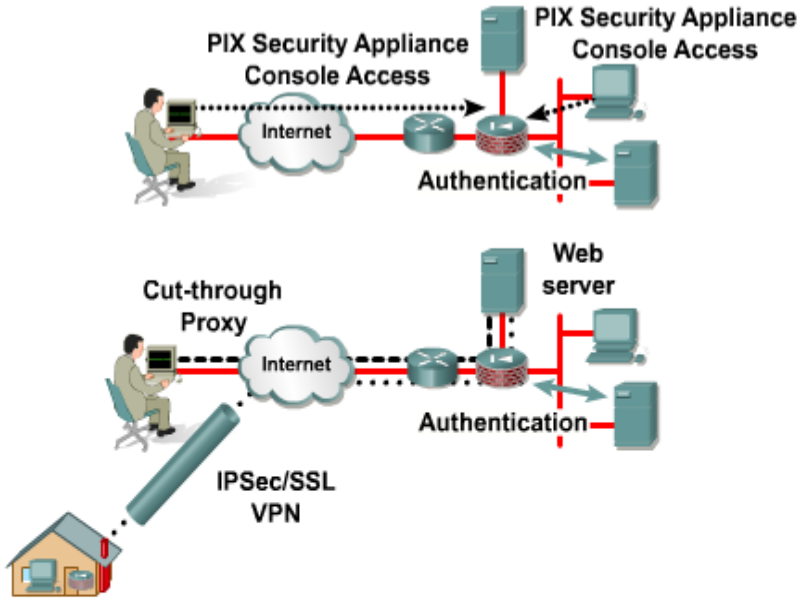
6.2 Introduction to PIX Security Appliance AAA Features

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Types of Authentication

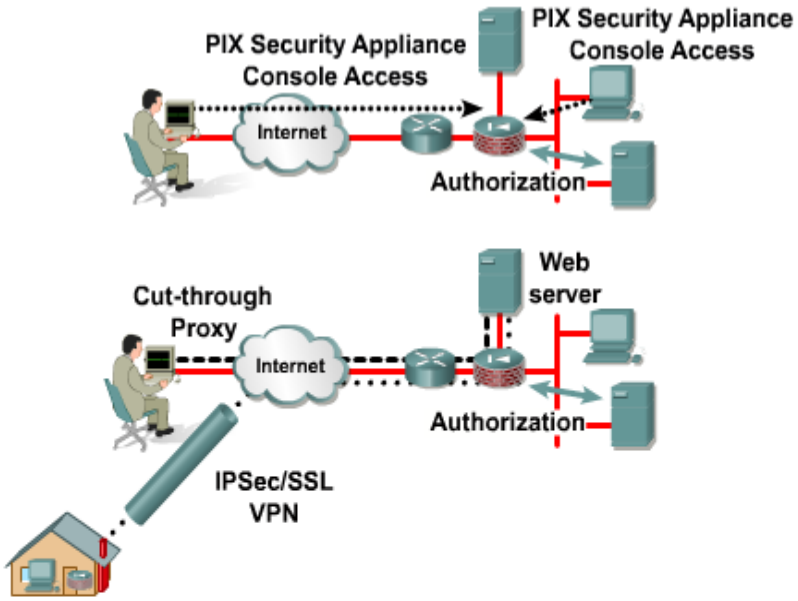


Types of authentication:

- Authenticate access to the security applicane
- Authenticate access through the security appliance
  - Cut-through proxy
- Authentication tunnel access
  - IPSec
  - SSL VPN

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Types of Authorization

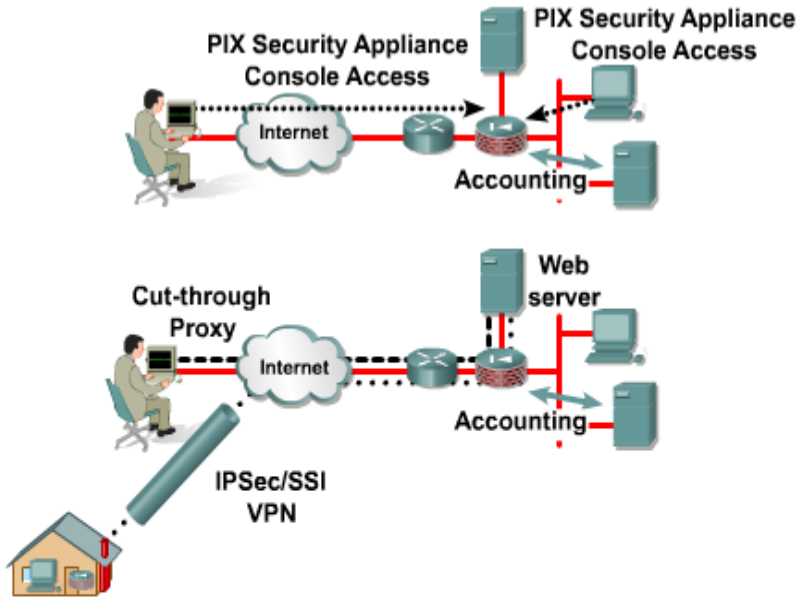


Types of authentication:

- Console access
  - specifies whether command execution is subject to authorization.
- Cut-through proxy
  - specifies what "throught" services are subject to authorization.
- Tunnel access
  - specifies what "tunnel" services are authorized.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Types of Accounting



Types of accounting:

- Accounting of pix security appliance console access
- Accounting of access through the pix security appliance
  - Cut-through proxy
- Accounting of tunnel connections
  - IPSec
  - SSL VPN

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems Networking Academy

Cisco.com

Module 6 – Configure Trust and Identity at Layer 3

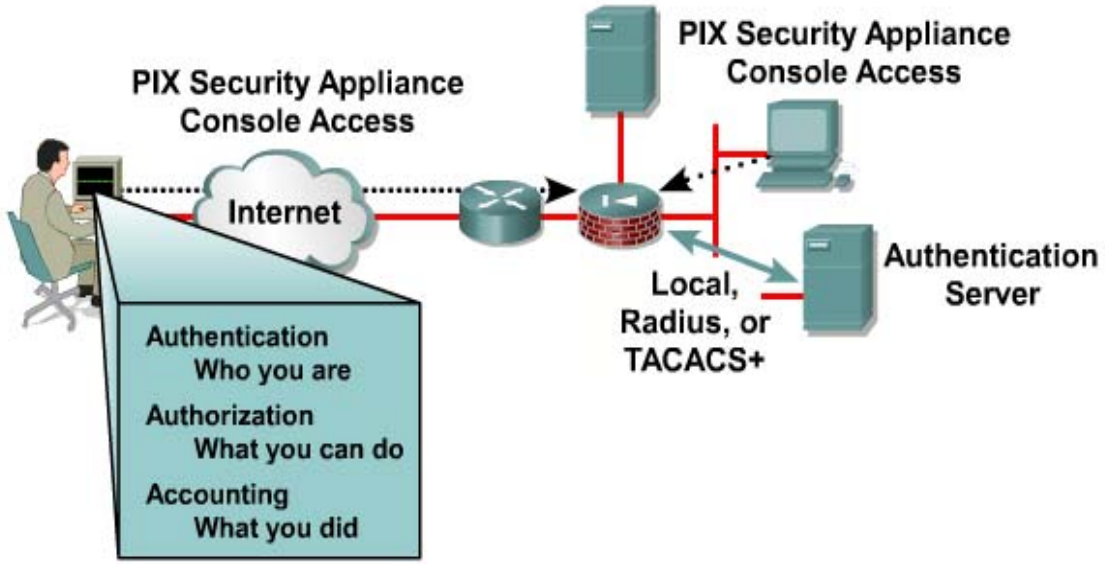
6.3 Configure AAA on the PIX Security Appliance

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Types of Access Authentication



Types of PIX security appliance console authentication

- Telnet
- SSH
- Serial
- Enable

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Authentication Configuration Steps

Access authentication configuration steps:

- **Specify an AAA server group.**

```
pixfirewall(config)# radius-server key string
```

- **Designate an authentication server.**

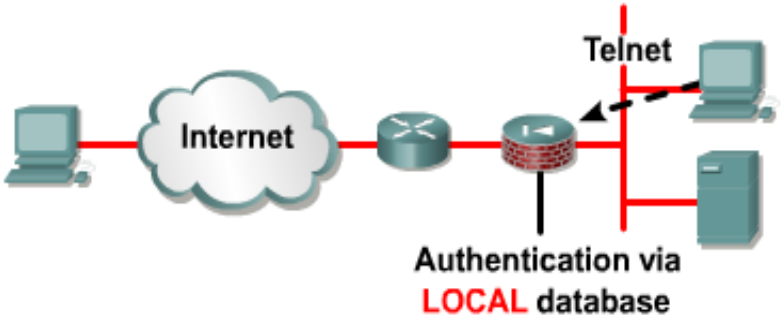
```
pixfirewall(config)# aaa-server server-tag
[(if_name)] host ip_address
```

- **Enable security appliance access authentication.**

```
pixfirewall(config)# aaa authentication [serial
enable | telnet | ssh | http] console server_tag
[LOCAL]
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Add Users to the Local User Database



pixfirewall(config)#

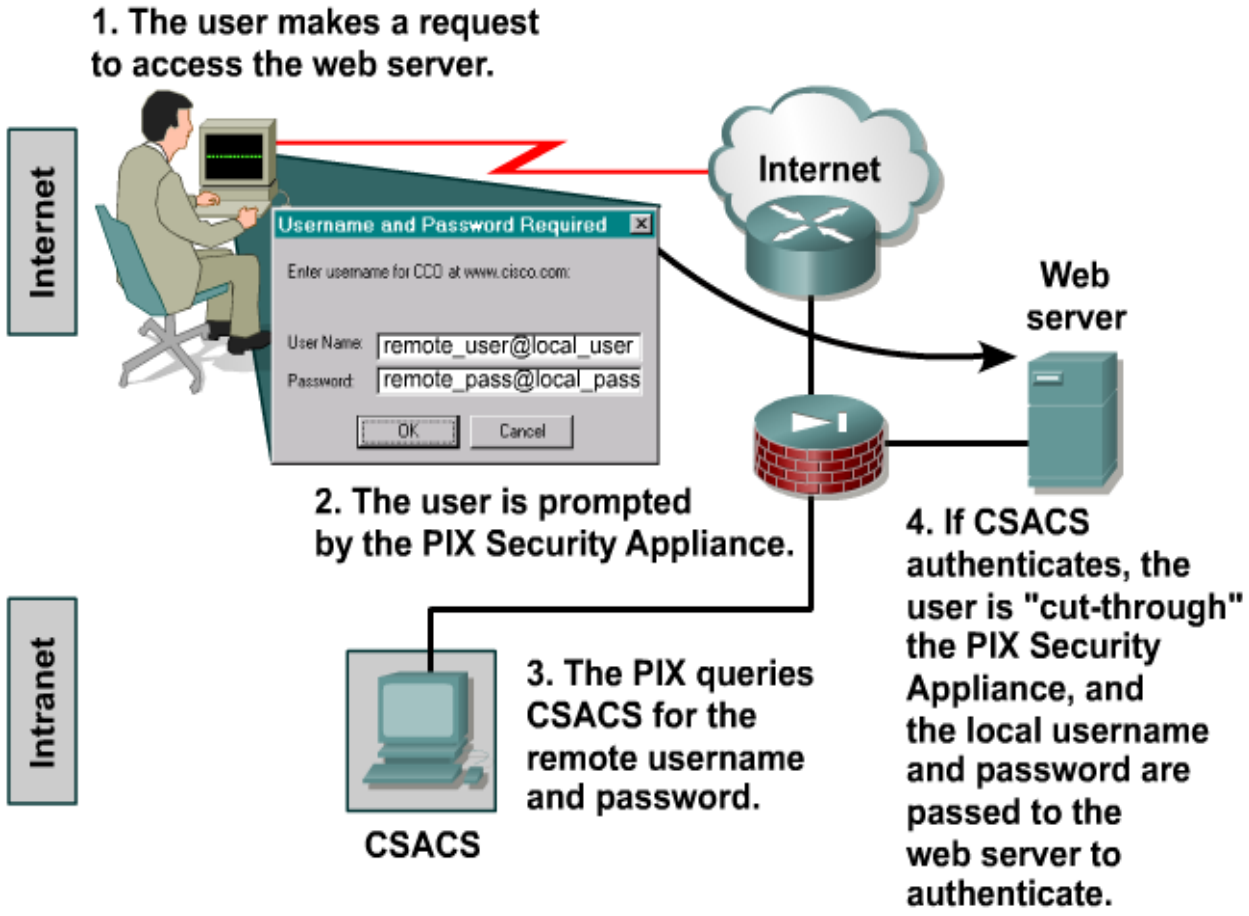
```
username name {nopassword | password password}
```

- Specify an username in the LOCAL database.
- Specify the LOCAL keyword in the authentication command.
- (Optional) Speciafy the maximum number of failed attempts after which a user is locked out

```
pixfirewall(config)# username admin1 password cisco123
pixfirewall(config)# aaa authentication telnet console LOCAL
```

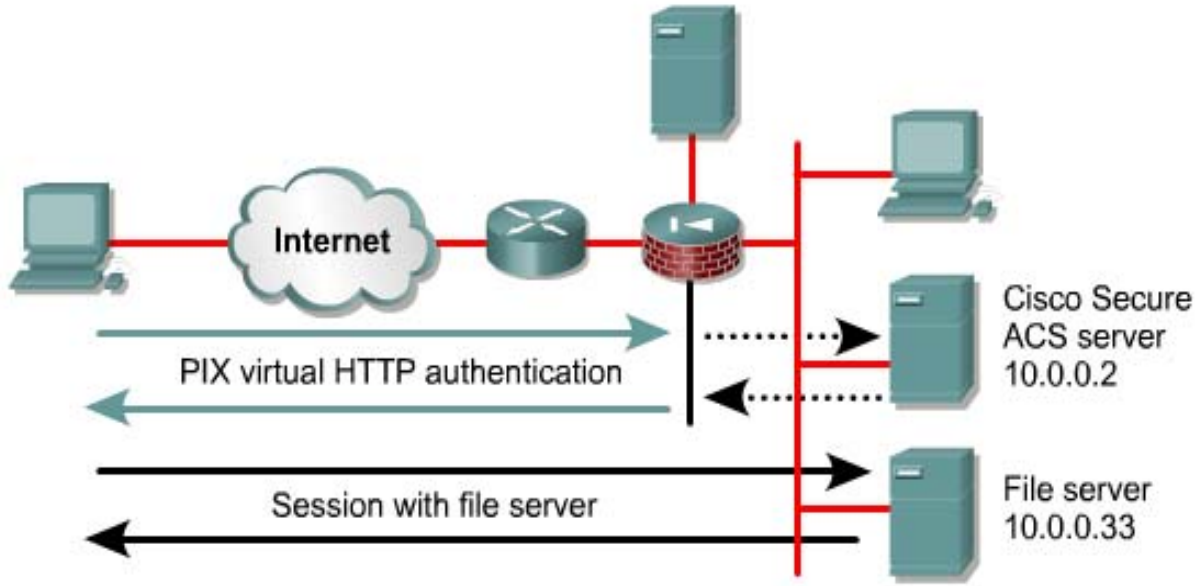
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cut-Through Proxy



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Authentication of Non-Telnet, FTP, or HTTP Traffic

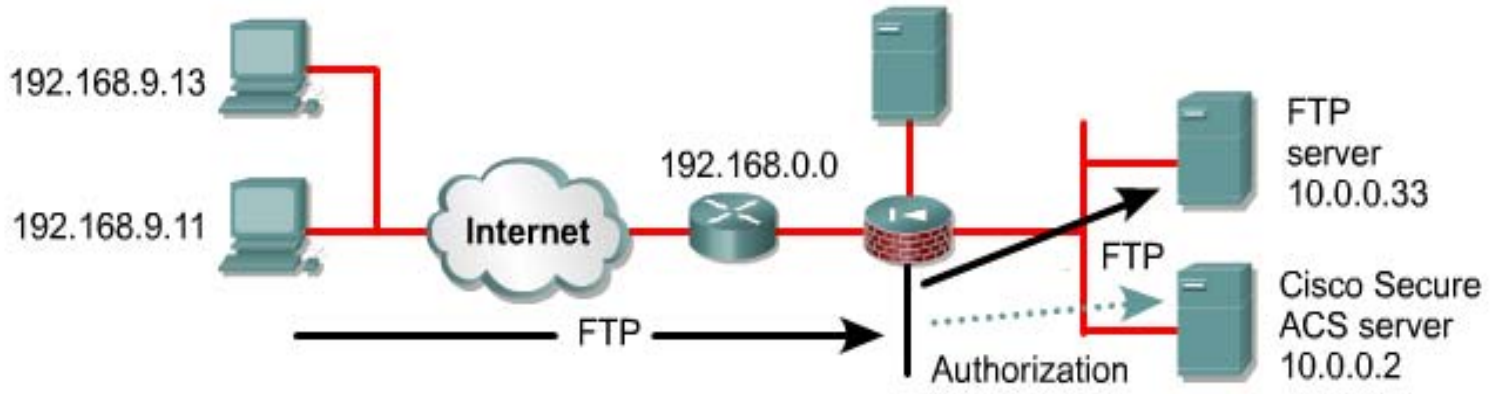


Authenticate to the PIX Security Appliance before accessing other services.

- Virtual Telnet
- Virtual HTTP

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

User Authorization

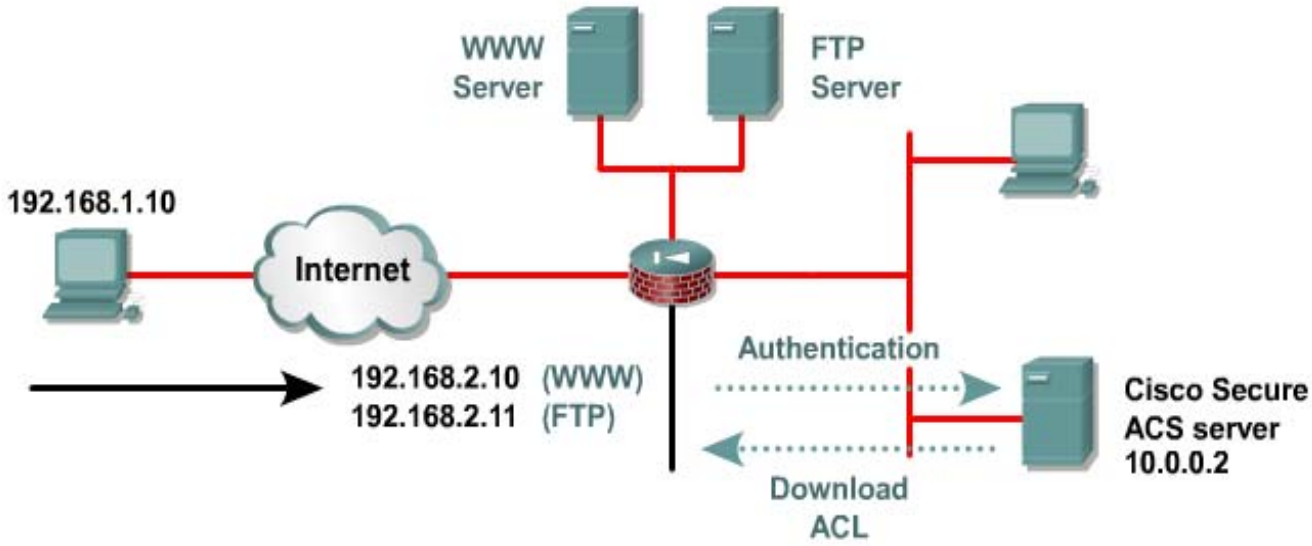


Two supported methods:

- Classic user authorization, where a TACACS+ AAA server is configured with rules and consulted for every connection
- Download of a per-user ACL from the RADIUS AAA server on demand

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Downloadable ACLs

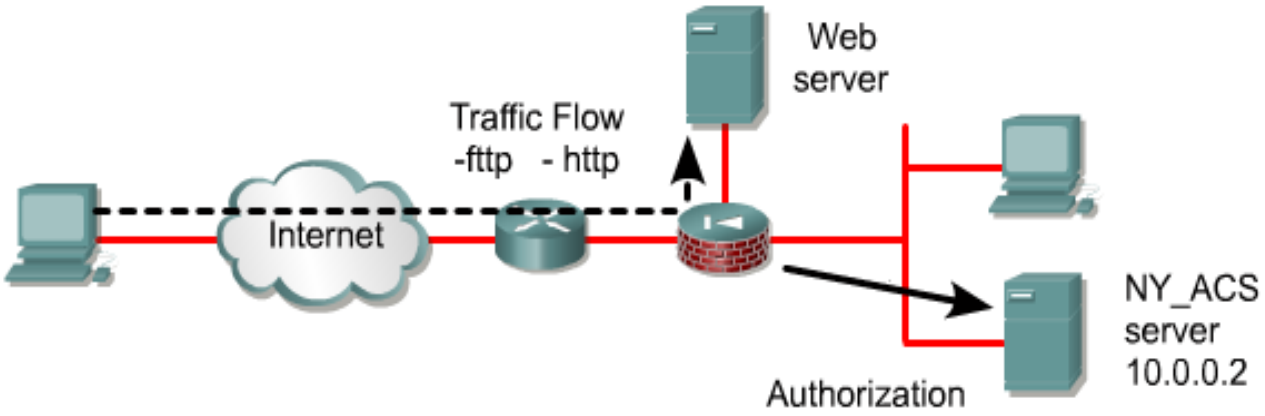


Downloadable ACLs:

- Authentication request to AAA server
- Authentication response containing ACL
- ACL download of a per-user, or per-group, ACL authorization

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Enable Accounting Match



pixfirewall(config)#

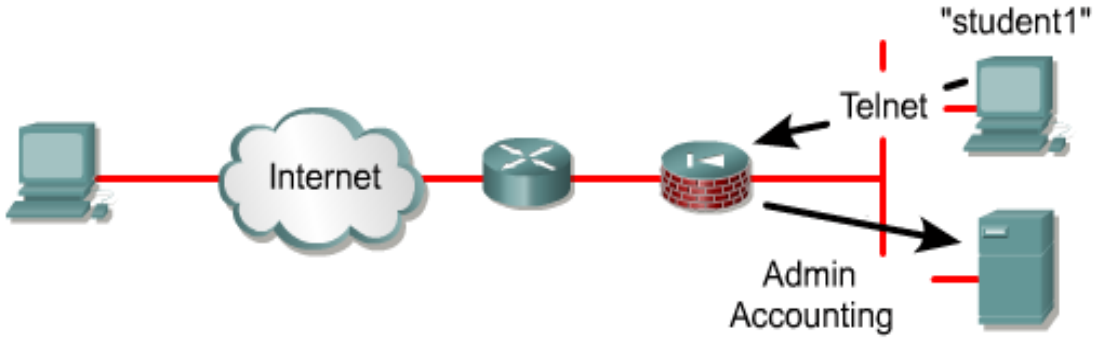
```
aaa accounting match acl_name interface_name server_tag
```

- Identify a traffic flow with an **access-list** command.
- Enable accounting of traffic matching **access-list** command statement.

```
pixfirewall(config)# access-list 110 permit tcp any host 192.168.2.10 eq ftp
pixfirewall(config)# access-list 110 permit tcp any host 192.168.2.10 eq www
pixfirewall(config)# aaa accounting match 110 outside NY_ACS
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Admin Accounting



pixfirewall(config)#

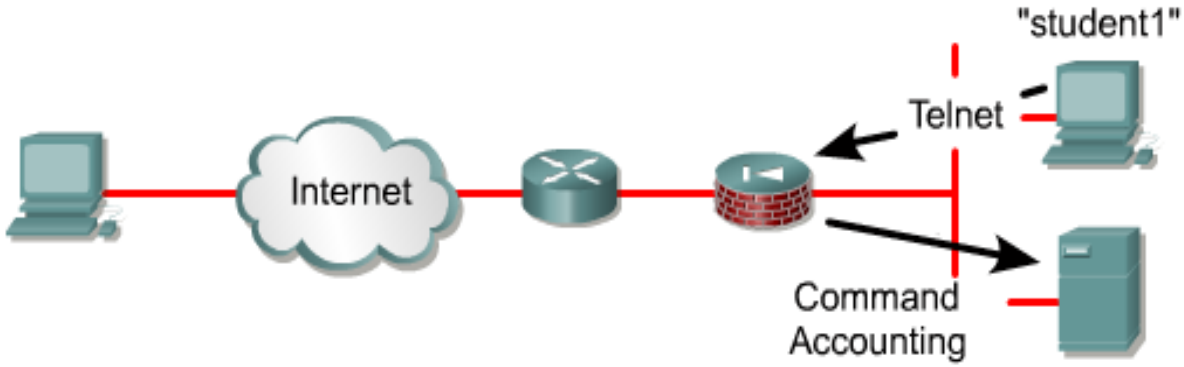
```
aaa accounting {http | serial| telnet | ssh | enable} console server-tag
```

- Enables or disables the generation of accounting records to mark the establishment and termination of admin sessions.
- Valid server group protocols are RADIUS and TACACS+.

```
pixfirewall(config)#  username student1 password cisco123
pixfirewall(config)#  aaa authentication telnet console LOCAL
pixfirewall(config)#  aaa accounting telnet console NY_ACS
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Command Accounting



pixfirewall(config)#

```
aaa accounting command [privilege_level] server-tag
```

- Enables or disables the generation of command accounting records for admin sessions.
- Valid server group protocol is TACACS+.

```
pixfirewall(config)#  aaa accounting command privilege 15 mytacacs
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se