CCNA 200-301, Volume 2

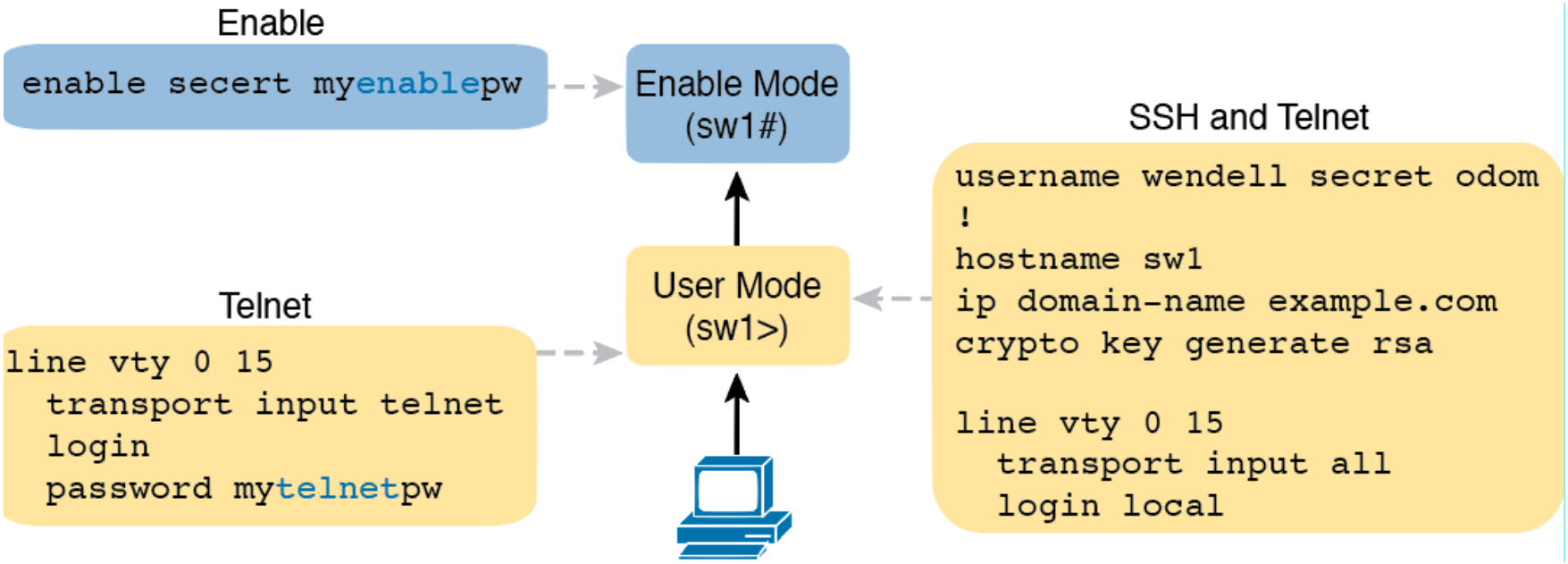
Chapter 5

Securing Network Devices

Objectives

- Explain the Role of Network Components
  - Next-generation firewalls and IPS
- Configure network devices for remote access using SSH
- Configure device access control using local passwords

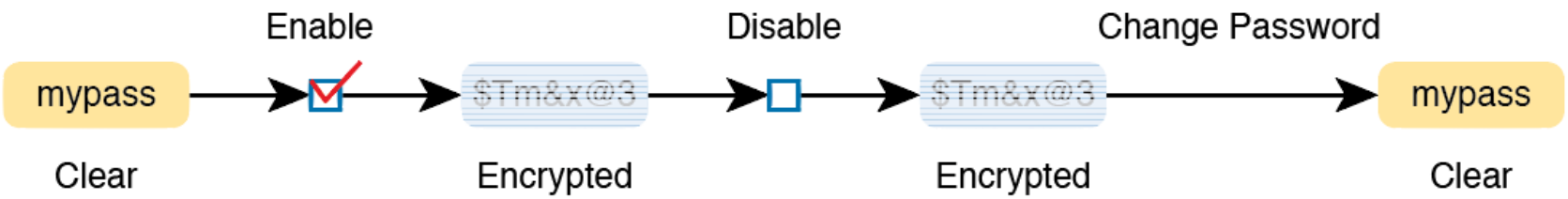
Example Login Security Configuration



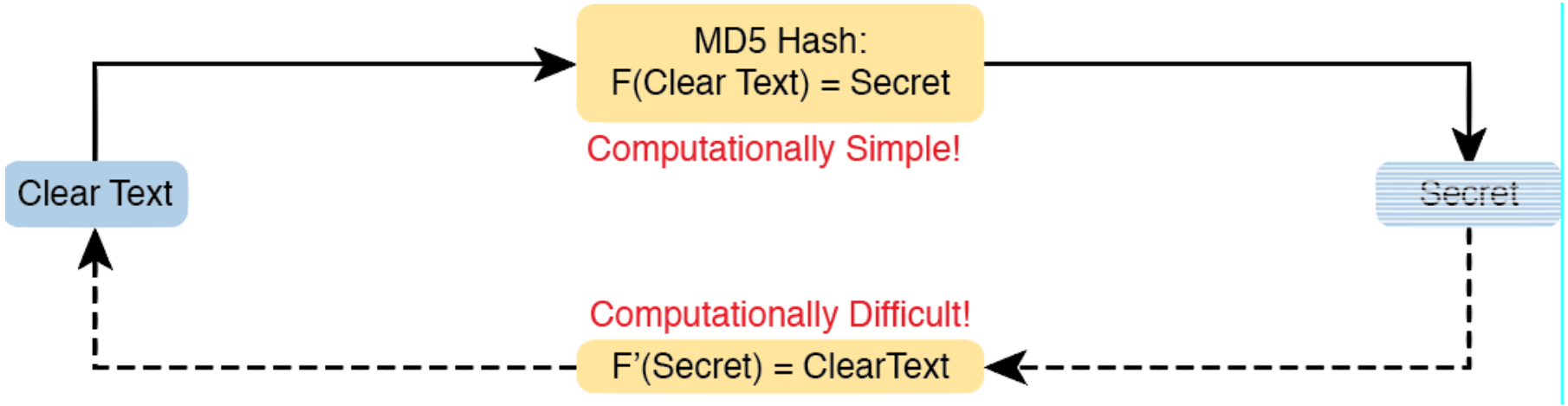
Encryption and the **service password-encryption** Command

```
Switch3# show running-config | section line con 0
line con 0
 password cisco
 login

Switch3# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch3(config)# service password-encryption
Switch3(config)# ^Z

Switch3# show running-config | section line con 0
line con 0
 password 7 070C285F4D06
 login
```

Encryption Is Immediate; Decryption Awaits Next Password Change



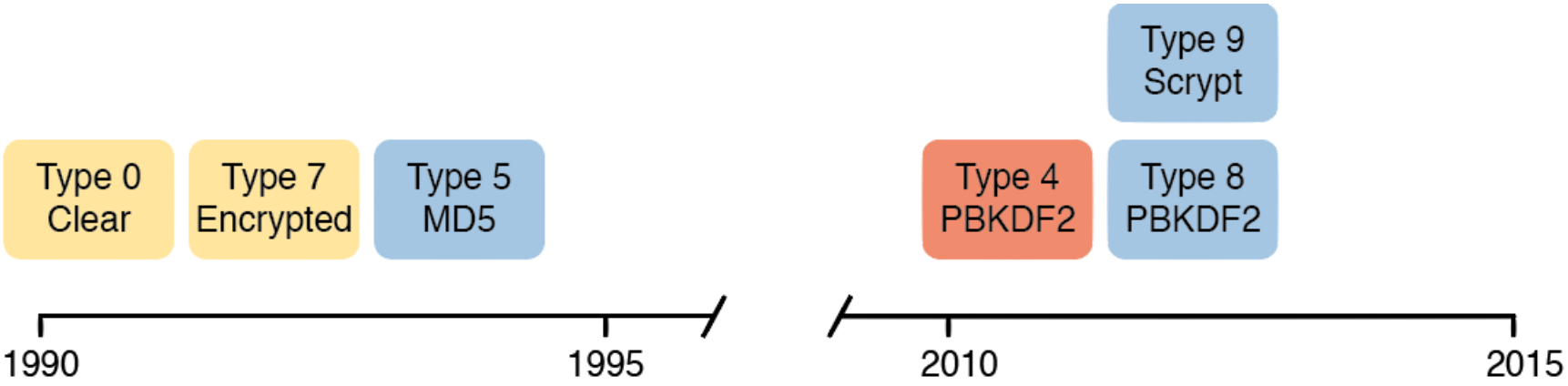
One-Way Nature of MD5 Hash to Create Secret



Creation of the **enable secret** Command

```
Switch3(config)# enable secret fred
Switch3(config)# ^Z
Switch3# show running-config | include enable secret

enable secret 5 $1$ZGMA$e8cmvkz4UjiJhVp7.maLE1

Switch3# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch3(config)# no enable secret
Switch3(config)# ^Z
```

Timeline of Encryptions/Hashes of Cisco IOS Passwords



Commands and Encoding Types for the **enable secret** Command

Command	Type	Algorithm
enable [algorithm-type md5] secret *password*	5	MD5
enable algorithm-type sha256 secret *password*	8	SHA-256
enable algorithm-type scrypt secret *password*	9	SHA-256

Cisco IOS Encoding Password “mypass1” as Type 9 (SHA-256)

```
R1# show running-config | include enable
enable secret 5 $1$ZSYj$725dBZmLUJ0nx8gFPTtTv0
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable algorithm-type scrypt secret mypass1
R1(config)# ^Z
R1#
R1# show running-config | include enable
enable secret 9 $9$II/EeKiRW91uxE$fwYuOE5EHoii16AWv2wSywkLJ/KNeGj8uK/24B0TVU6
R1#
```

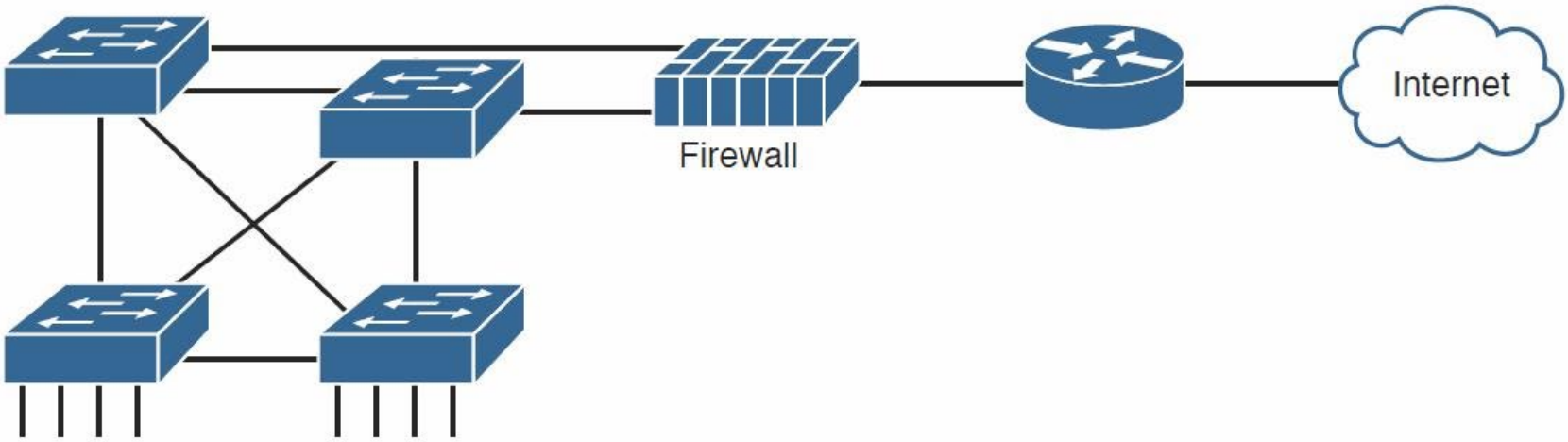
Commands and Encoding Types for the **username secret** Command

Command	Type	Algorithm
username *name* [algorithm-type md5] secret *password*	5	MD5
username *name* algorithm-type sha256 secret *password*	8	SHA-256
username *name* algorithm-type scrypt secret *password*	9	SHA-256

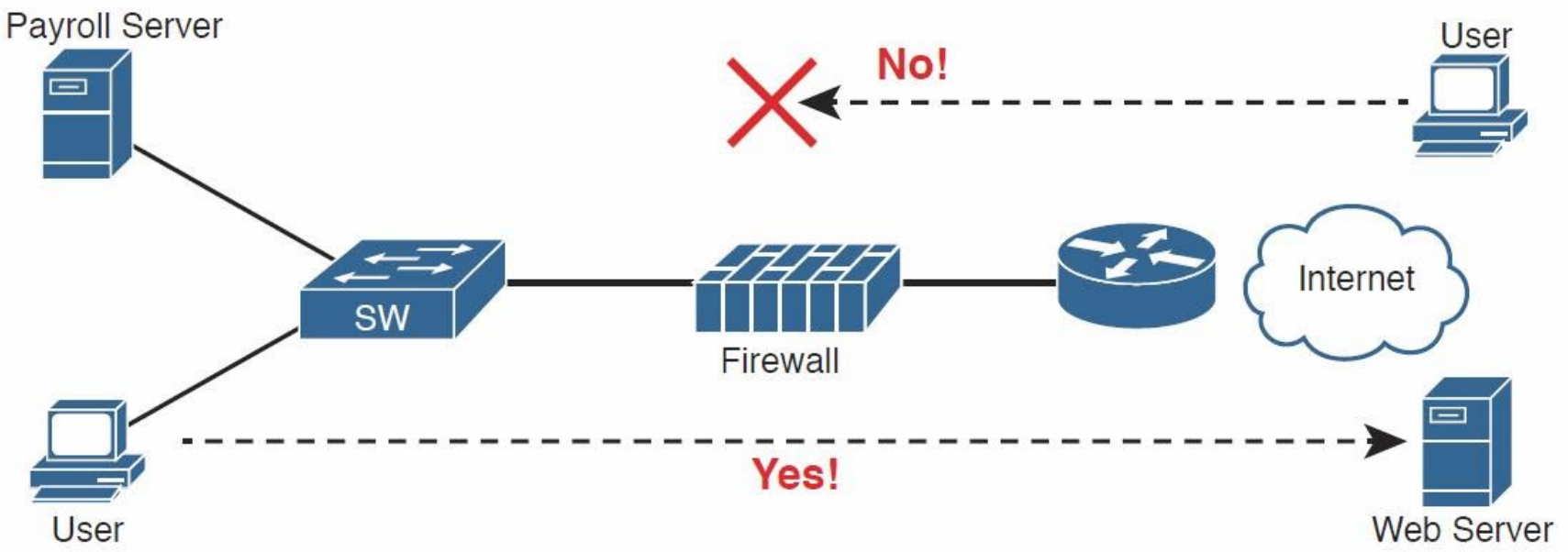
vty Access Control Using the **access-class** Command

```
line vty 0 4
 login
 password cisco
 access-class 3 in
!
! Next command is a global command that matches IPv4 packets with
! a source address that begins with 10.1.1.
 access-list 3 permit 10.1.1.0 0.0.0.255
```

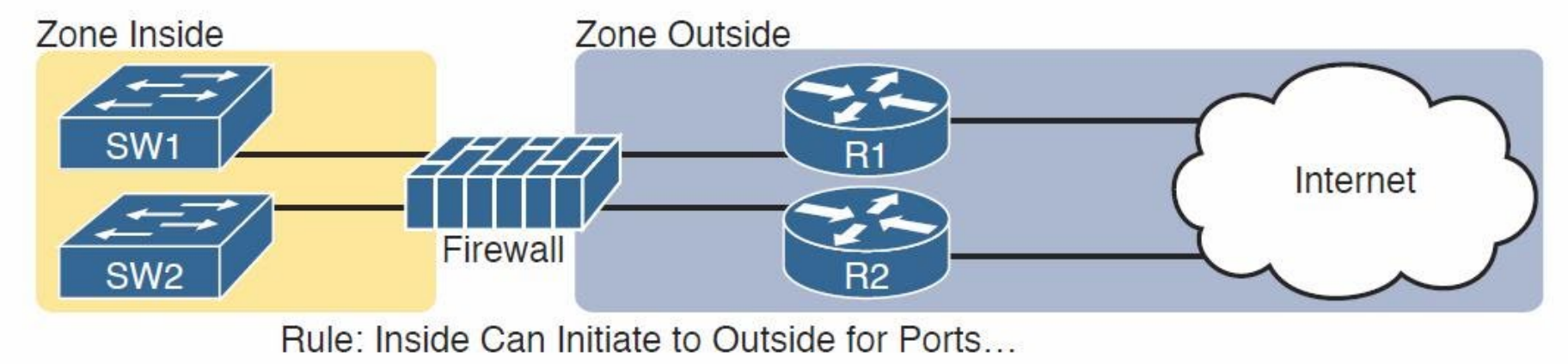
Firewall as Positioned in the Packet Forwarding Path



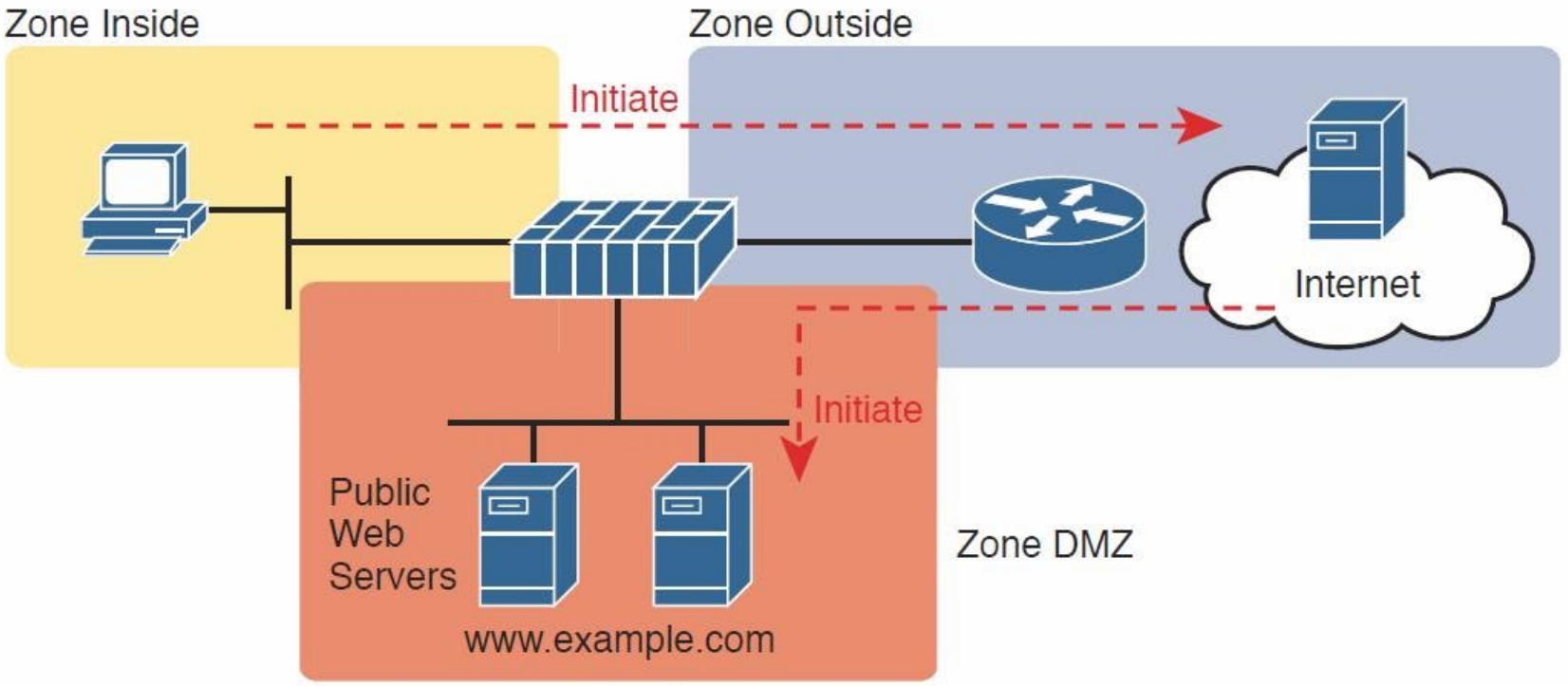
Allowing Outbound Connections and Preventing Inbound Connections



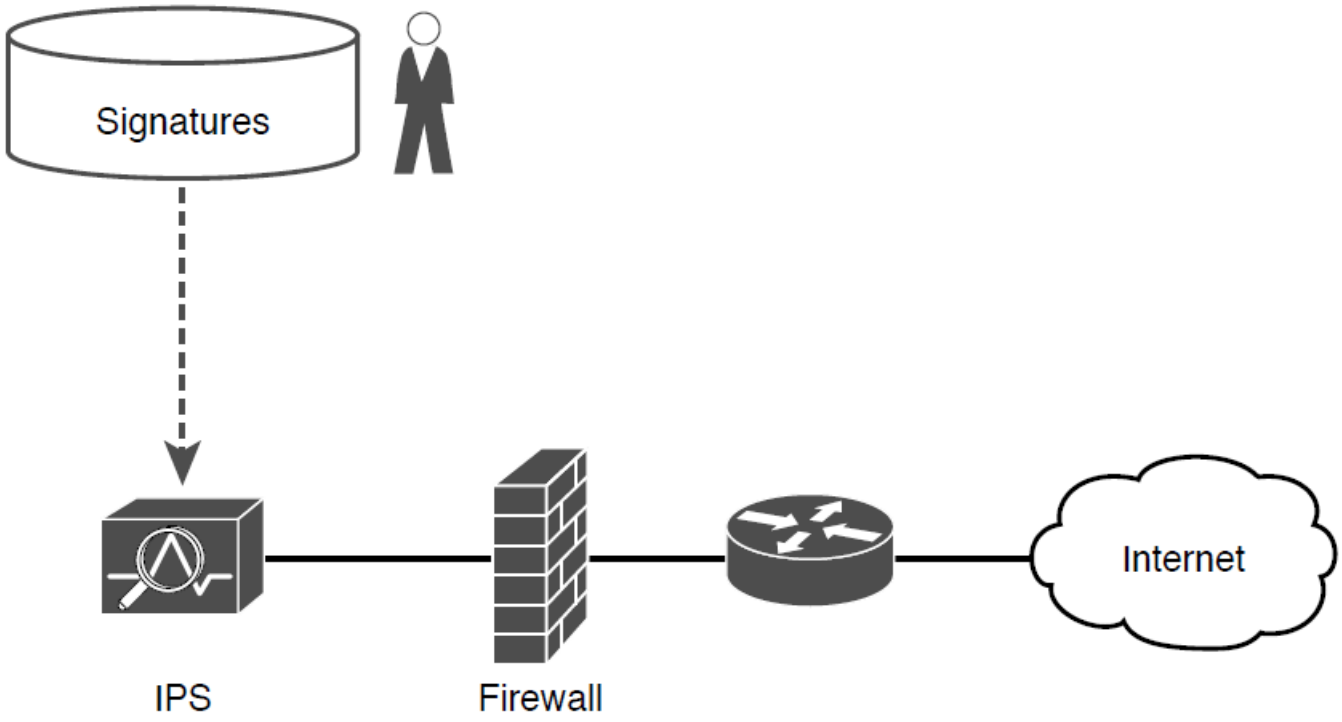
Using Security Zones with Firewalls



Using a DMZ for Enterprise Servers That Need to Be Accessible from the Internet



IPS and Signature Database



Next-Generation Firewall with Next-Generation IPS Module