Cisco Systems
Networking Academy

Cisco.com

Network Security 2

Module 2 – Configure Network Intrusion Detection and Prevention

CCNA CISCO CERTIFIED

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

Högskolan Halmstad

Learning Objectives

Cisco.com

–2.1 Cisco IOS Intrusion Prevention System

–2.2 Configure Attack Guards on the PIX Security Appliance

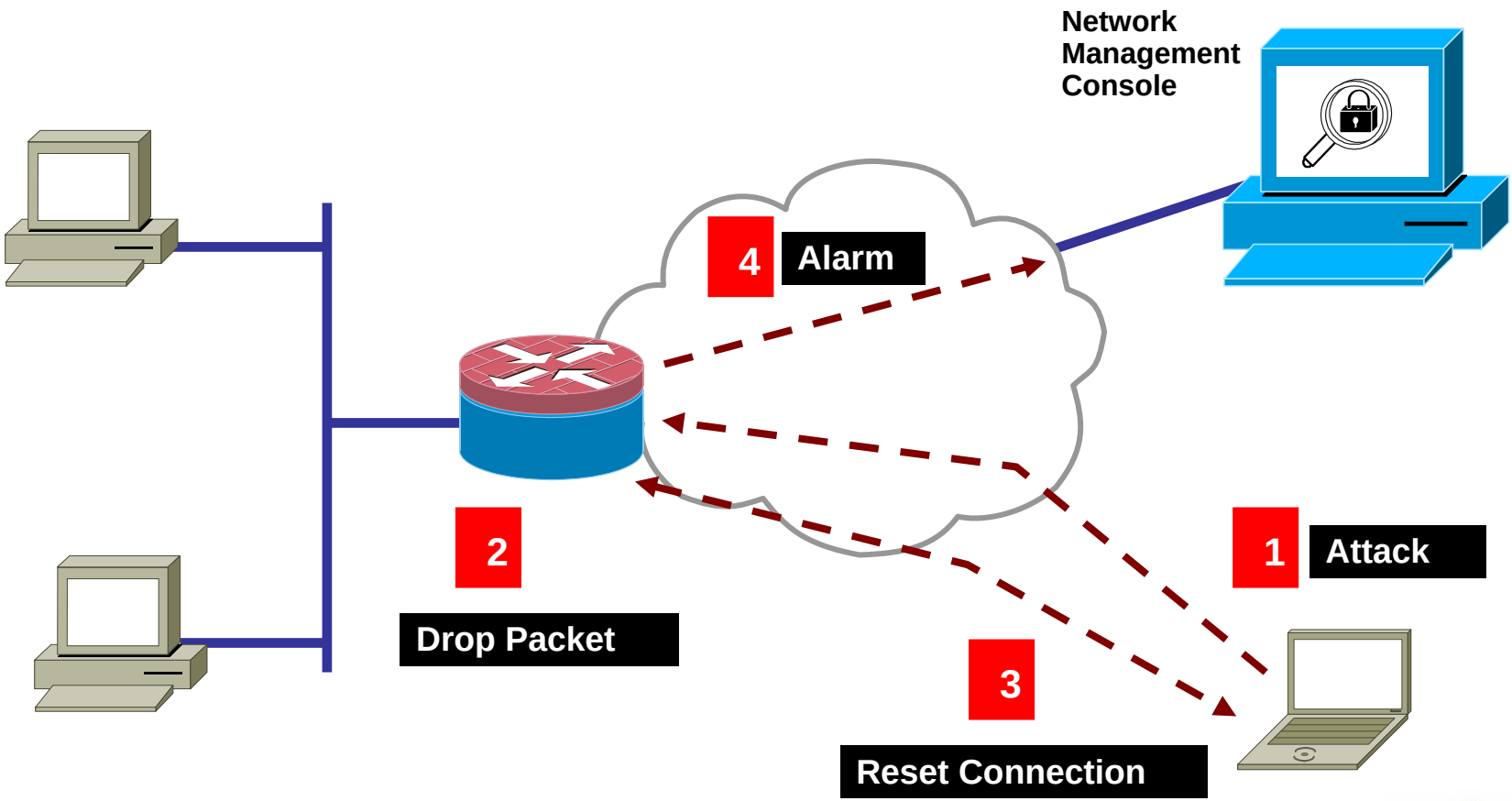
–2.3 Configure Intrusion Prevention on the PIX Security Appliance

–2.4 Configure Shunning on the PIX Security Appliance

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

Cisco IOS Intrusion Prevention System

Cisco.com



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

Configuration Tasks

- Install Cisco IOS IPS on the router.
  - Specify location of the Signature Definition File (SDF).
  - Create an IPS rule.
  - Attach a policy to a signature (Optional).
  - Apply IPS rule at an interface.
- Configure Logging using Syslog or SDEE.
- Verify the configuration.

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

Specify Location of SDF

Cisco.com

Router (config)#

```
ip ips sdf location url
```

- (Optional) Specifies the location in which the router will load the SDF, attack-drop.sdf.
- If this command is not issued, the router will load the default, built-in signatures.

```
Router(config)# ip ips sdf location
  disk2:attack-drop.sdf
```

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

Create an IPS Rule

Cisco.com

```
Router (config)#
```

```
ip ips name ips-name [list acl]
```

- **Creates an IPS rule.**

```
Router(config)# ip ips name MYIPS
```

- **Creates an IPS rule named MYIPS that will be applied to an interface.**

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

Attach a policy to a given signature(Optional)

Cisco.com

```
Router (config)#
```

```
ip ips signature signature-id [:sub-signature-id]
  {delete | disable | list acl-list}
```

- **Attaches a policy to a given signature.**

```
Router(config)# ip ips signature 1000 disable
```

- **Disables signature 1000 in the signature definition file.**

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

Apply an IPS Rule at an Interface

Cisco.com

```
Router (config-if)#
```

```
ip ips ips-name {in | out}
```

- **Applies an IPS rule at an interface.**

```
Router(config-if)# ip ips MYIPS in
```

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

Upgrade to Latest SDF


```
Router (config)#
ip ips name ips-name
```

- **Creates an IPS rule.**

```
Router (config)#
no ip ips sdf builtin
```

- **Instructs the router not to load the built-in signatures.**

```
Router (config)#
ip ips fail closed
```

- **Instructs the router to drop all packets until the signature engine is built and ready to scan traffic.**

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

Upgrade to Latest SDF(Cont.)

Router (config-if)#

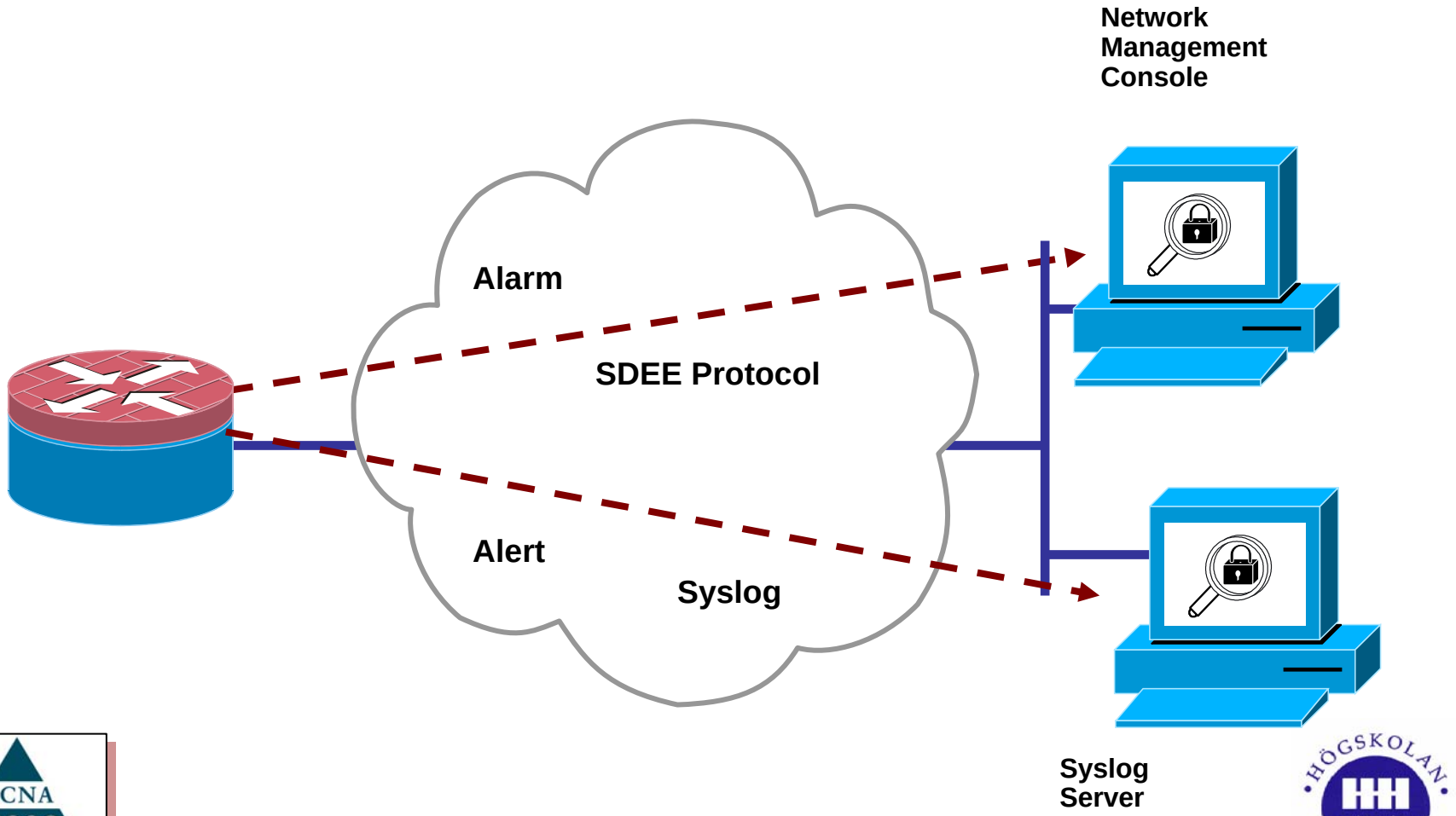
```
ip ips ips-name {in | out} [list acl]
```

- **Applies an IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.**

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

Monitoring Cisco IOS IPS Signatures

Cisco.com



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

SDEE Benefits

- Vendor Interoperability – SDEE will become the standard format for all vendors to communicate events to a network management application. This lowers the cost of supporting proprietary vendor formats and potentially multiple network management platforms.
- Secured transport – The use of HTTP over SSL or HTTPS ensures that data is secured as it traverses the network

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

Set Notification Type

Cisco.com

```
Router (config)#
```

```
ip ips notify [log | sdee]
```

- **Sets notification type**

```
Router(config)# ip ips notify sdee
Router(config)# ip ips notify log
```

```
Router (config)#
```

```
ip sdee events num_of_events
```

- **Sets the maximum number of SDEE events that can be stored in the event buffer.**

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

show Commands

Cisco.com

```
Router#
show ip ips configuration
```

- **Verifies that Cisco IOS IPS is properly configured.**

```
Router#
show ip ips signatures [detailed]
```

- **Verifies signature configuration, such as signatures that have been disabled.**

```
Router#
show ip ips interface
```

- **Display the interface configuration**

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

clear Commands

Cisco.com

```
Router#
clear ip ips configuration
```

- **Remove all intrusion prevention configuration entries, and release dynamic resources.**

```
Router#
clear ip ips statistics
```

- **Reset statistics on packets analyzed and alarms sent**

```
Router#
clear ip sdee {events | subscriptions}
```

- **Clear SDEE events or subscriptions.**

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

debug Commands

Cisco.com

```
Router# debug ip ips timers
Router# debug ip ips object-creation
Router# debug ip ips object-deletion
Router# debug ip ips function trace
Router# debug ip ips detailed
Router# debug ip ips ftp-cmd
Router# debug ip ips ftp-token
Router# debug ip ips icmp
Router# debug ip ips ip
Router# debug ip ips rpc
Router# debug ip ips smtp
Router# debug ip ips tcp
Router# debug ip ips tftp
Router# debug ip ips udp
```

- **Instead of no, undebug may be used**

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

Cisco Systems
Networking Academy

Cisco.com

Module 2 – Configure Network Intrusion Detection and Prevention

2.2 Configure Attack Guards on the PIX Security Appliance

CCNA CISCO CERTIFIED

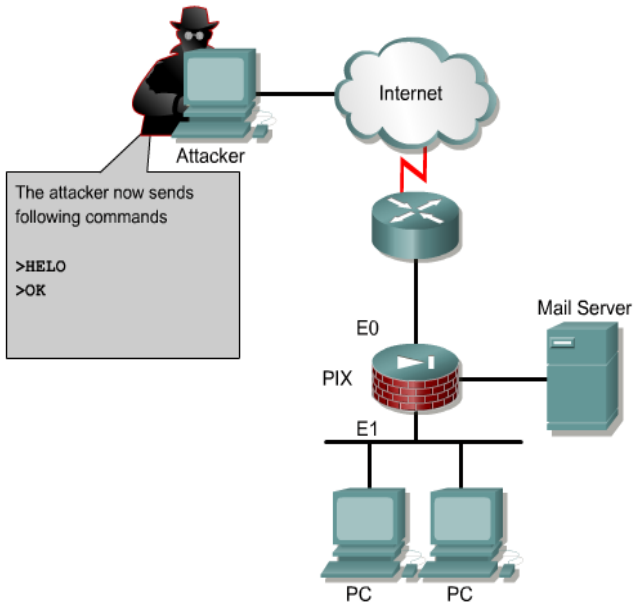
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

Mail Guard

Cisco.com

- Provides a safe conduit for Simple Mail Transfer Protocol (SMTP) connections from the outside to an inside e-mail server
- Enables administrators to deploy a mail server within the internal network, without it being exposed to known security problems that exist within some mail server implementations
- Only the SMTP commands specified in RFC 821 section 4.5.1 are allowed to a mail server
- By default, the Cisco Secure PIX Security Appliance inspects port 25 connections for SMTP traffic
- SMTP servers using ports other than port 25 must use the fixup protocol smtp command



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

Mail Guard

pixfirewall (config)#

```
fixup protocol smtp port [-port]
```

- **Defines ports on which to activate Mail Guard (default = 25)—Only allows RFC 821, section 4.5.1 commands: HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT.**
- **If disabled, all SMTP commands are allowed through the firewall—Potential mail server vulnerabilities are exposed.**

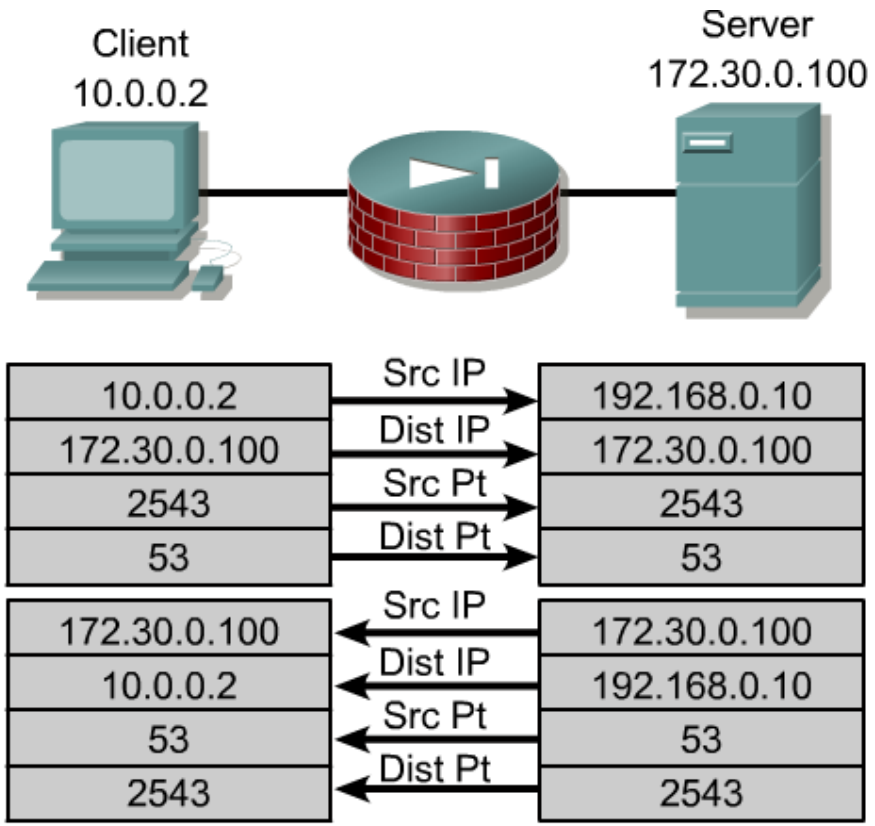
```
pixfirewall(config)# fixup protocol smtp 2525
pixfirewall(config)# fixup protocol smtp 2625-2635
pixfirewall(config)# no fixup protocol smtp 25
```

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

DNS Guard

Cisco.com

- DNS Guard is always on.
- After the client does a DNS request, a dynamic conduit allows UDP packets to return from the DNS server. The default UDP timer expires in two minutes.
- The DNS server response is recognized by the firewall, which closes the dynamic UDP conduit immediately. The PIX Security Appliance does not wait for the UDP timer to expire.



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

FragGuard and Virtual Re-assembly

- The FragGuard and Virtual Re-assembly feature has the following characteristics:
  - Is on by default.
  - Verifies each fragment set for integrity and completeness.
  - Tags each fragment in a fragment set with the transport header.
  - Performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the PIX Security Appliance.
  - Uses Syslog to log fragment overlapping and small fragment offset anomalies.

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

fragment Command

pixfirewall (config)#

```
fragment size database-limit [interface]
```

- Sets the maximum number of packets in the fragment database.

pixfirewall (config)#

```
fragment chain chain-limit [interface]
```

- Specifies the maximum number of packets into which a full IP packet can be fragmented.

pixfirewall (config)#

```
fragment timeout seconds [interface]
```

- Specifies the maximum number of seconds that the PIX Security Appliance waits before discarding a packet that is waiting to be reassembled.

```
pixfirewall(config)# fragment size 1
pixfirewall(config)# fragment chain 1
```

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

AAA Flood Guard

Cisco.com

pixfirewall (config)#

```
floodguard enable | disable
```

- **Reclaims attacked or overused AAA resources to help prevent DoS attacks on AAA services (default = enabled).**

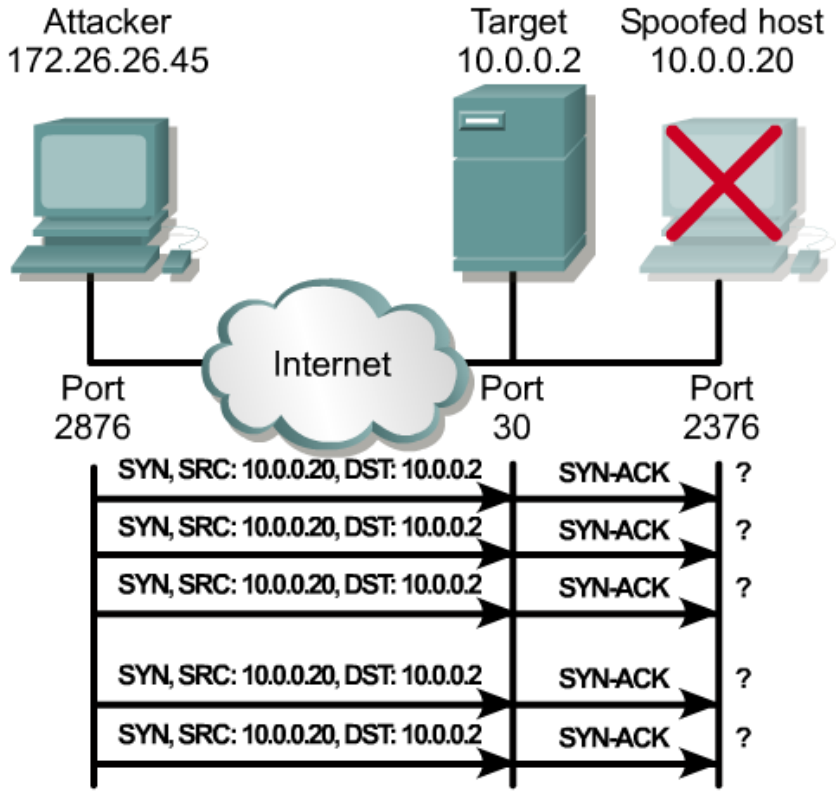
```
pixfirewall(config)# floodguard enable
```

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

SYN Flood Attack

Cisco.com

- The attacker spoofs a nonexistent source IP address and floods the target with SYN packets.
- The target responds to the SYN packets by sending SYN-ACK packets to the spoofed hosts.
- The target overflows its port buffer with embryonic connections and stops responding to legitimate requests.



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

SYN Flood Guard Configuration

pixfirewall (config)#

```
static [(prenat_interface, postnat_interface)]
  mapped_address | interface real_address [dns][netmask
  mask][norandomseq][connection_limit [em_limit]]
```

- For inbound connections:
  - Use the em_limit to limit the number of embryonic connections.
  - Set the limit to a number lower than the server can handle.

pixfirewall (config)#

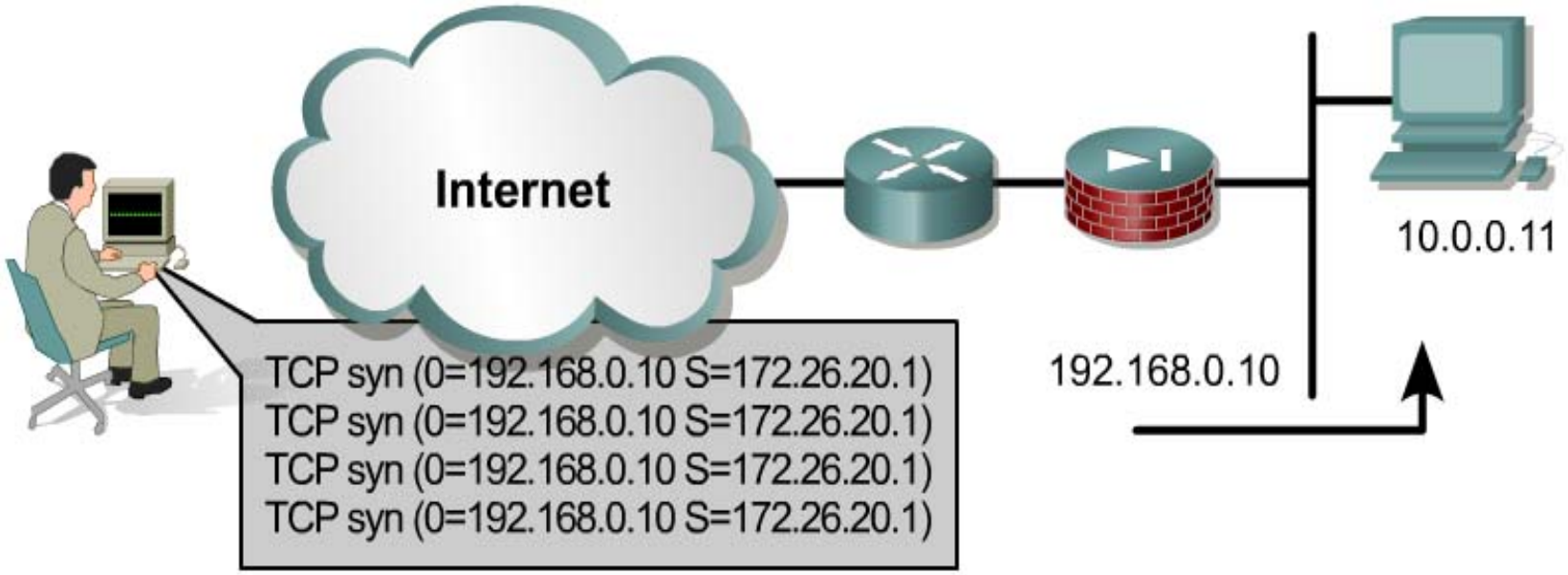
```
nat [(if-name)]id address [netmask [outside] [dns]
  [norandomseq] [timeout hh:mm:ss] [conn_limit [em_limit]]]
```

- For outbound connections:
  - Use the em_limit to limit the number of embryonic connections.
  - Set the limit to a number lower than the server can handle.

```
pixfirewall(config)# nat (inside) 1 0 0 0 10000
pixfirewall(config)# static (inside,outside) 192.168.0.11
  172.16.0.2 0 1000
```

TCP Intercept

Cisco.com




```
pixfirewall(config)# static (inside,outside) 192.168.0.10
  10.0.0.11 netmask 255.255.255.255 1000 100
```

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

Cisco Systems
Networking Academy

Cisco.com

Module 2 – Configure Network Intrusion Detection and Prevention

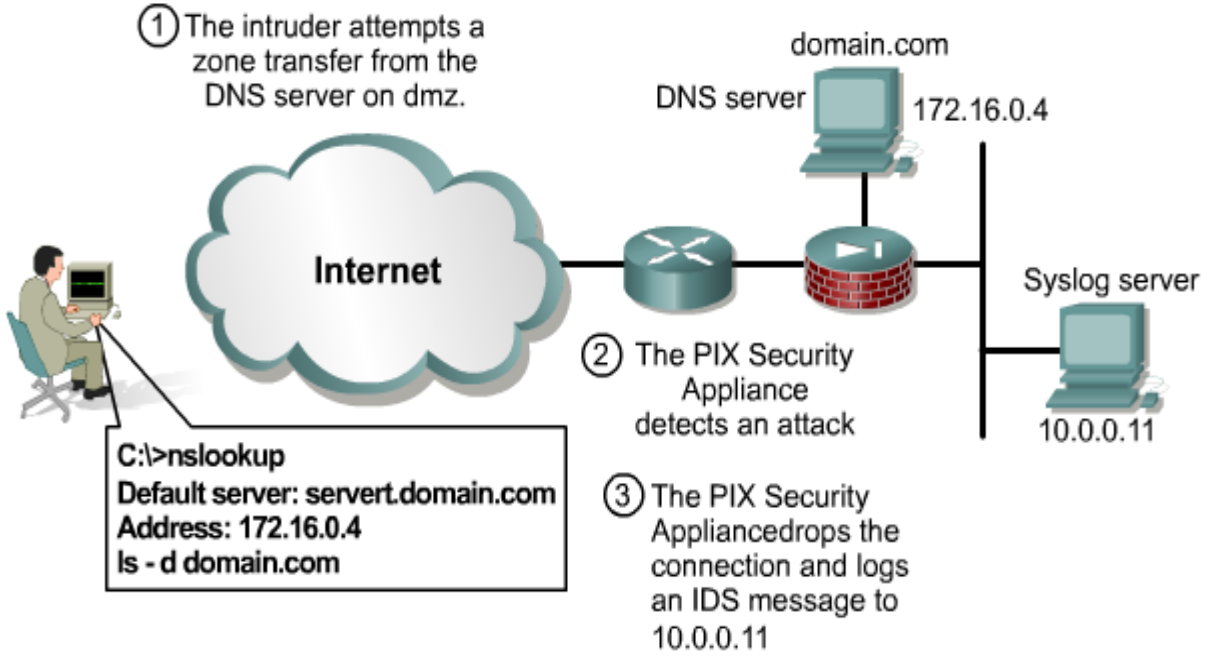
2.3 Configure Intrusion Prevention on the PIX Security Appliance

CCNA CISCO CERTIFIED

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

Högskolan Halmstad

PIX IDS



The steps taken during intrusion detection on a PIX Security Appliance.

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

Configure IDS

pixfirewall(config)#

```
ip audit name audit_name info [action [alarm] [drop] [reset]]
```

- **Creates a policy for informational signatures.**

pixfirewall(config)#

```
ip audit name audit_name attack [action [alarm] [drop] [reset]]
```

- **Creates a policy for attack signatures.**

pixfirewall(config)#

```
ip audit interface if_name audit_name
```

- **Applies a policy to an interface.**

```
pixfirewall(config)# ip audit name ATTACKPOLICY attack action
  alarm reset
pixfirewall(config)# ip audit interface outside ATTACKPOLICY
```

- **When the PIX Security Appliance detects an attack signature on its outside interface, it reports an event to all configured Syslog servers, drops the offending packet, and closes the connection if it is part of an active connection.**

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

Specify Default Actions for Signatures

Cisco.com

pixfirewall(config)#

```
ip audit attack [action [alarm] [drop] [reset]]
```

- **Specifies the default actions for attack signatures.**

pixfirewall(config)#

```
ip audit info [action [alarm] [drop] [reset]]
```

- **Specifies the default actions for informational signatures.**

```
pixfirewall(config)# ip audit info action alarm drop
```

- **When the PIX Security Appliance detects an info signature, it reports an event to all configured Syslog servers and drops the offending packet.**

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

Disable Intrusion Detection Signatures

Cisco.com

pixfirewall(config)#

```
ip audit signature signature_number
 disable
```

– Excludes a signature from auditing.

```
pixfirewall(config)# ip audit signature
 6102 disable
```

- **Disables signature 6102.**

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

Cisco Systems Networking Academy

Cisco.com

Module 2 – Configure Network Intrusion Detection and Prevention

2.4 Configure Shunning on the PIX Security Appliance

CCNA CISCO CERTIFIED

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

Högskolan Halmstad

shun Command

Cisco.com

pixfirewall(config)#

shun *src_ip* [*dst_ip sport dport* [*protocol*]]

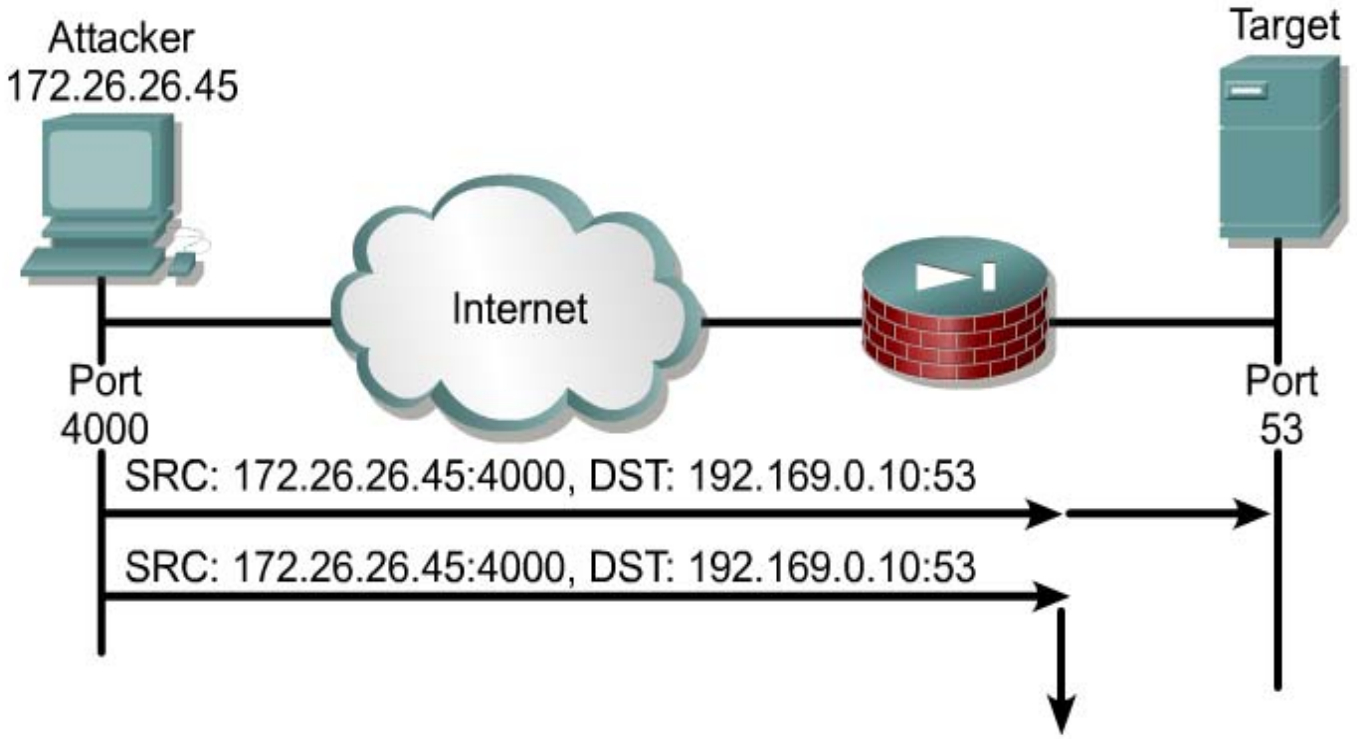
– Applies a blocking function to an interface under attack.

```
pixfirewall(config)# shun 172.26.26.45
```

- **No further traffic from 172.26.26.45 is allowed.**

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

Shunning an Attacker




```
pixfirewall(config)# shun 172.26.26.45
  192.168.0.10 4000 53
```

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