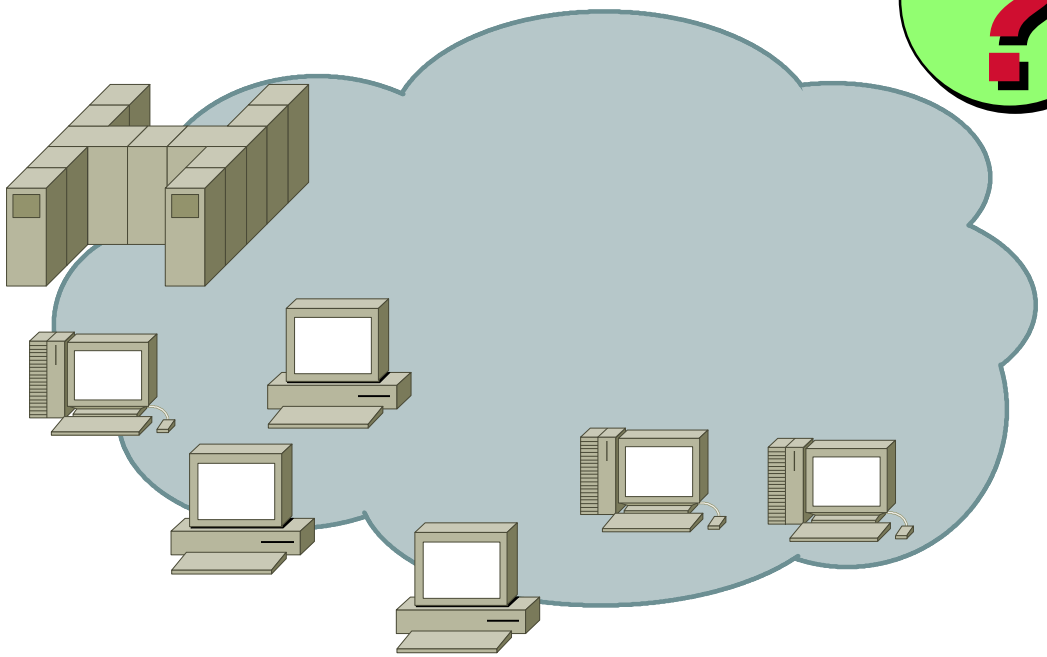
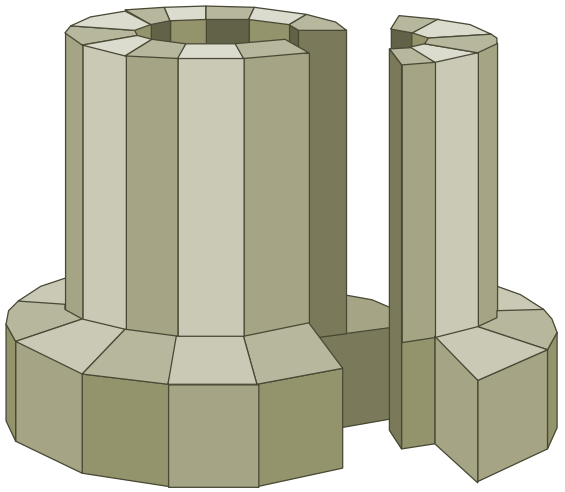
Example Scenario

Protect the email server



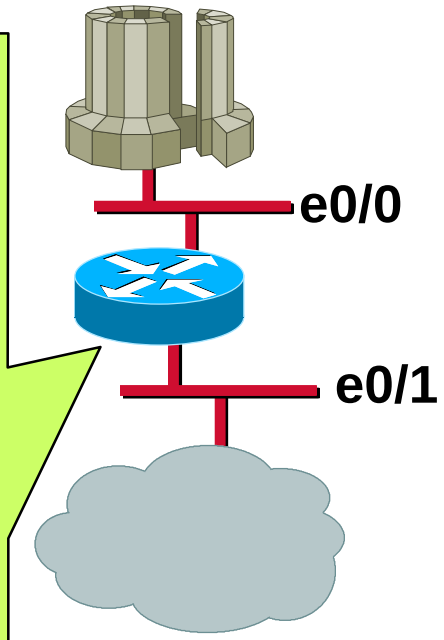


SMTP Host

CISCO SYSTEMS

Cisco IOS with an Access List

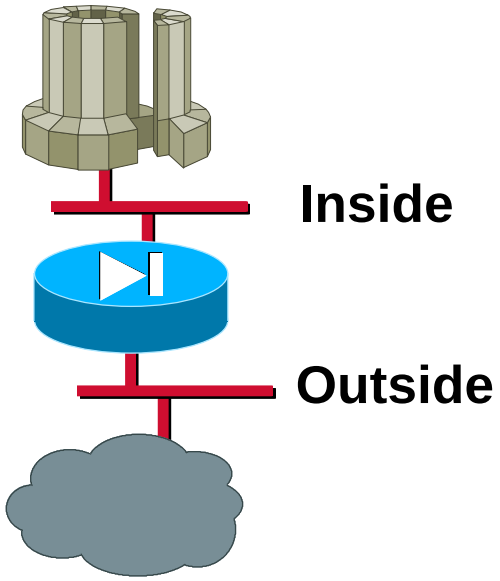
```
interface ethernet 0/0
 ip address 172.16.1.100  255.255.0.0
!
interface ethernet 0/1
 ip address 172.17.1.100  255.255.0.0
 ip access-group 111 in
no ip unreachables
no ip redirects
!
access-list 111 permit tcp any host 172.16.1.1 eq smtp
access-list 111 permit tcp any host 172.16.1.1 established
access-list 111 permit icmp any host 172.16.1.1
```



Cisco Systems

PIX

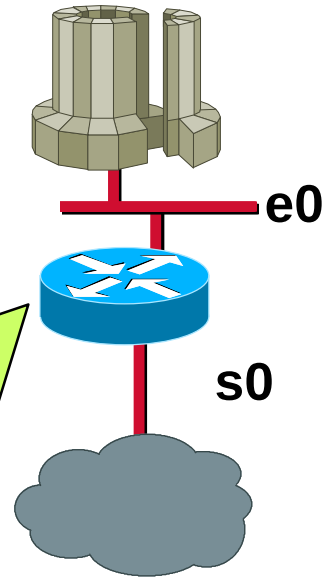
```
PIX Version 4.0.7
interface ethernet outside 10baset
interface ethernet inside 10baset
ip address inside 10.1.1.101  255.255.0.0
ip address outside 172.17.1.100  255.255.0.0
arp timeout 14400
mailhost 172.17.1.12  10.1.1.2
conduit 172.17.1.12  25 tcp 0.0.0.0  0.0.0.0
conduit 172.17.1.12  110 tcp 0.0.0.0  0.0.0.0
conduit 172.17.1.12  113 tcp 0.0.0.0  0.0.0.0
```



Cisco Systems

Cisco IOS Firewall Feature Set

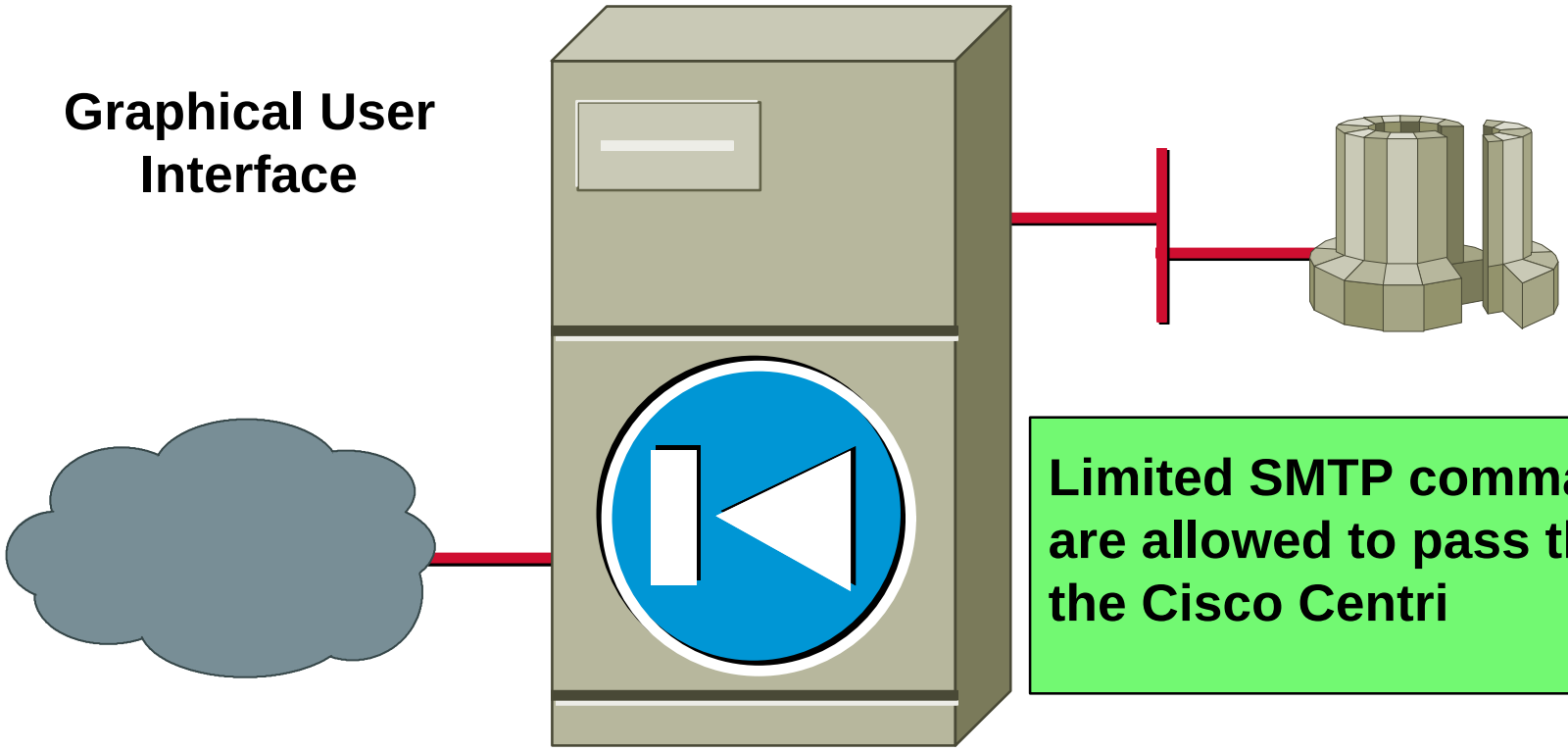
```
logging 172.16.27.131
ip inspect audit-trail
ip inspect dns-timeout 10
ip inspect tcp idle-time 60
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tcp timeout 3600
!
interface Ethernet 0
  ip address 172.16.1.100 255.255.0.0
  ip inspect myfw in
!
interface Serial 0
  ip address 172.19.139.1 255.255.255.248
  ip access-group 111 in
!
access-list 111 permit tcp any host 172.16.1.1 eq smtp
access-list 111 permit tcp any host 172.16.1.1 eq pop3
access-list 111 permit tcp any host 172.16.1.1 eq ident
```



Cisco Systems

Cisco Centri Firewall

Graphical User Interface



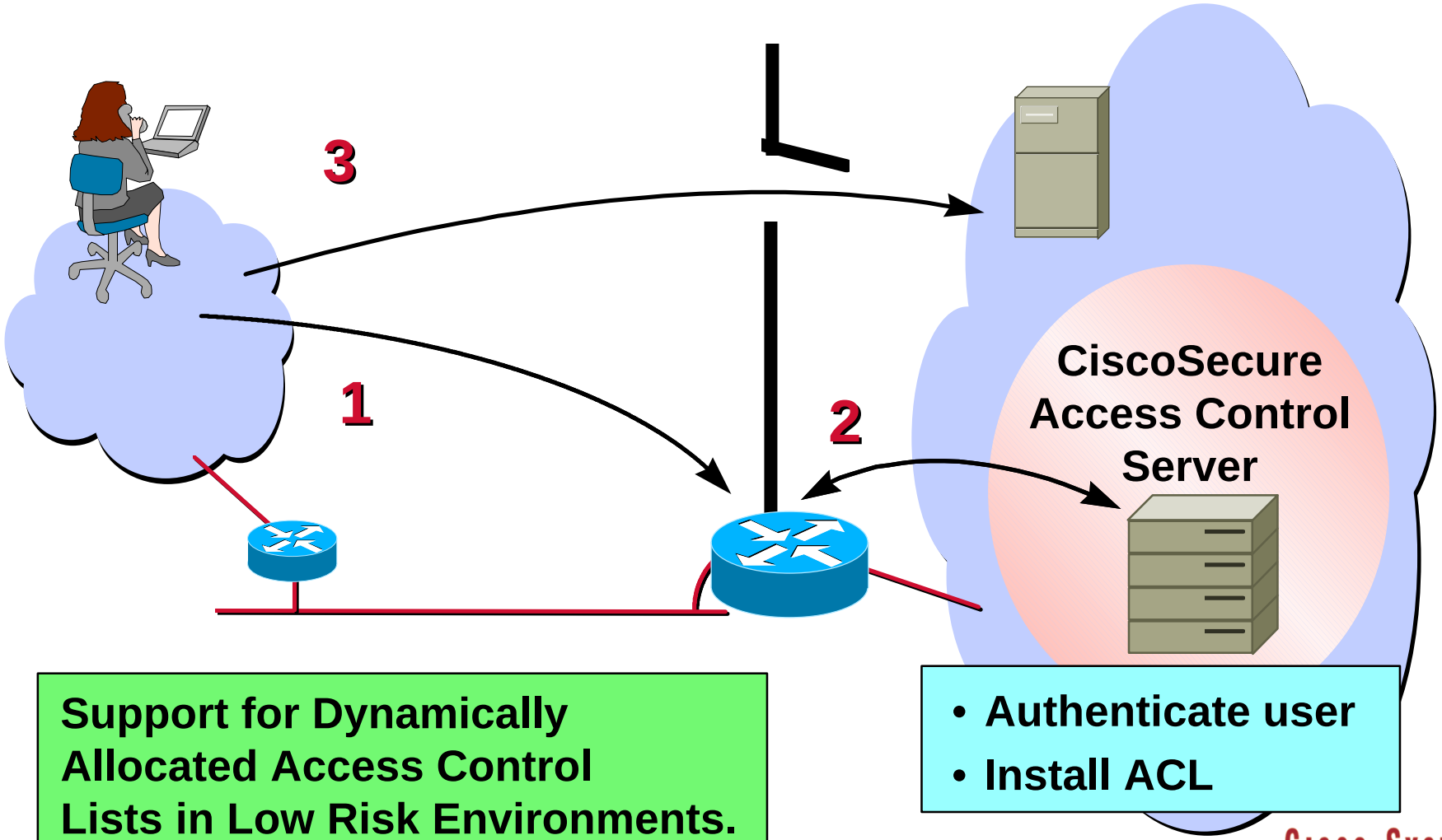
Limited SMTP commands are allowed to pass through the Cisco Centri

More Mechanisms to Enforce Your Security Policy

- Cisco IOS Lock and Key
- Hot Standby Router Protocol
- Spanning Tree Bridging
- Local Director
- Distributed Director

Cisco Systems

Cisco IOS—Lock and Key

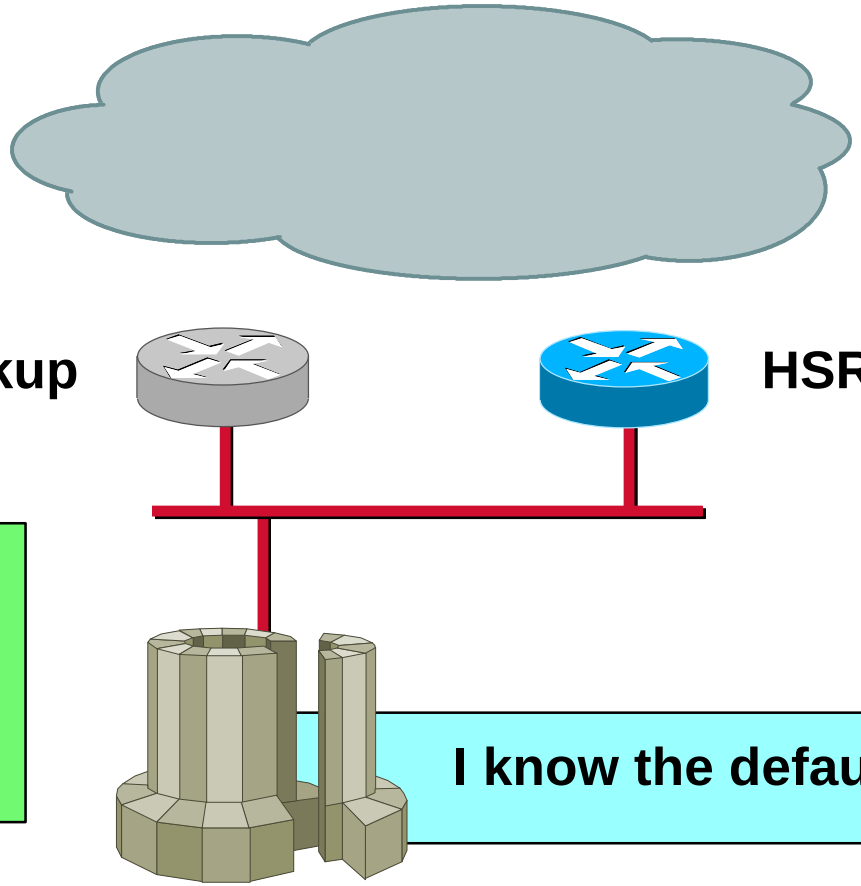


Support for Dynamically Allocated Access Control Lists in Low Risk Environments.

- Authenticate user
- Install ACL

Cisco Systems

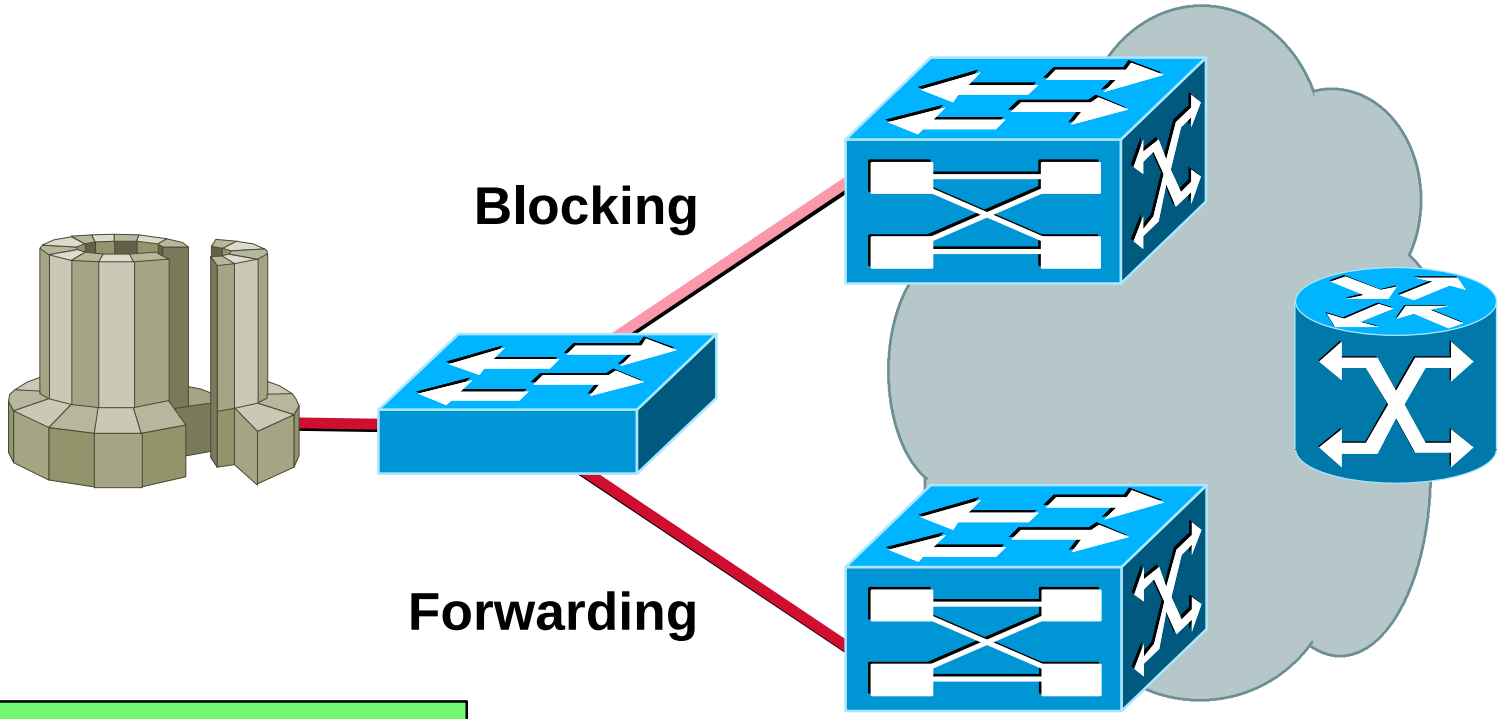
Hot Standby Router Protocol



Maintain a network link to a vital resource.

Cisco Systems

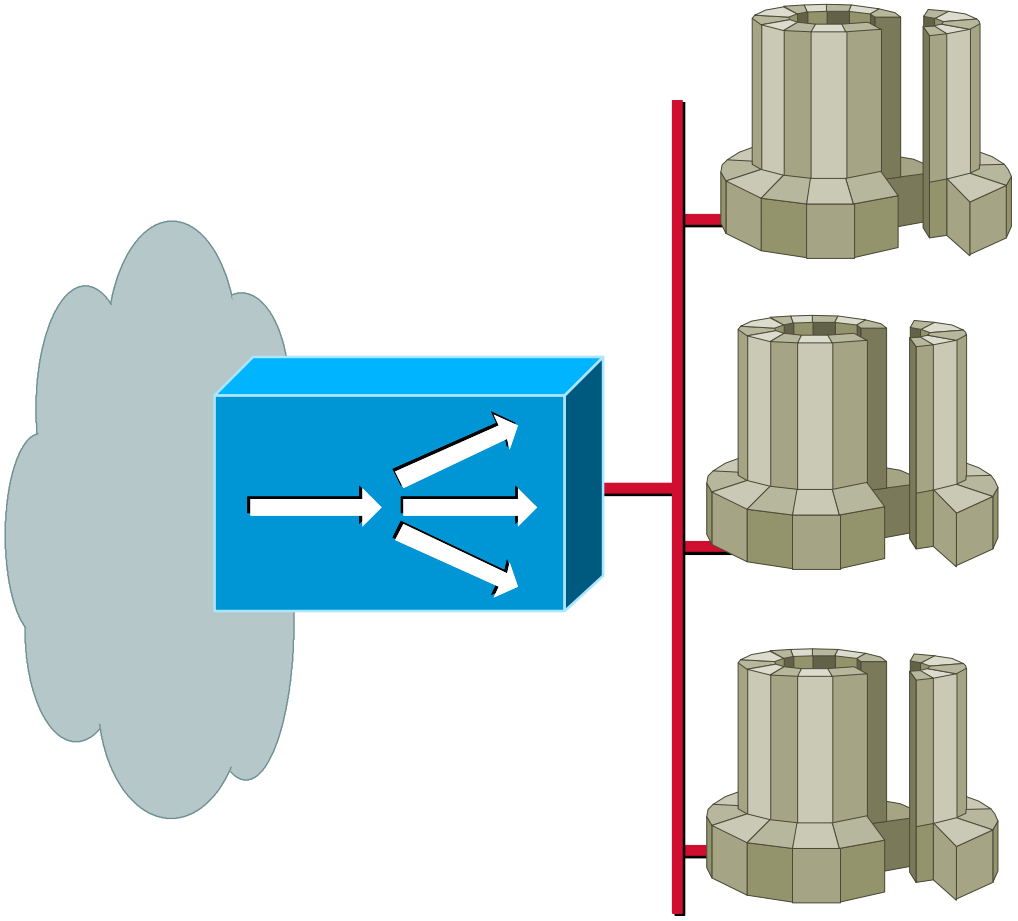
Spanning Tree Bridging



Maintain a network link to a vital resource

Local Director

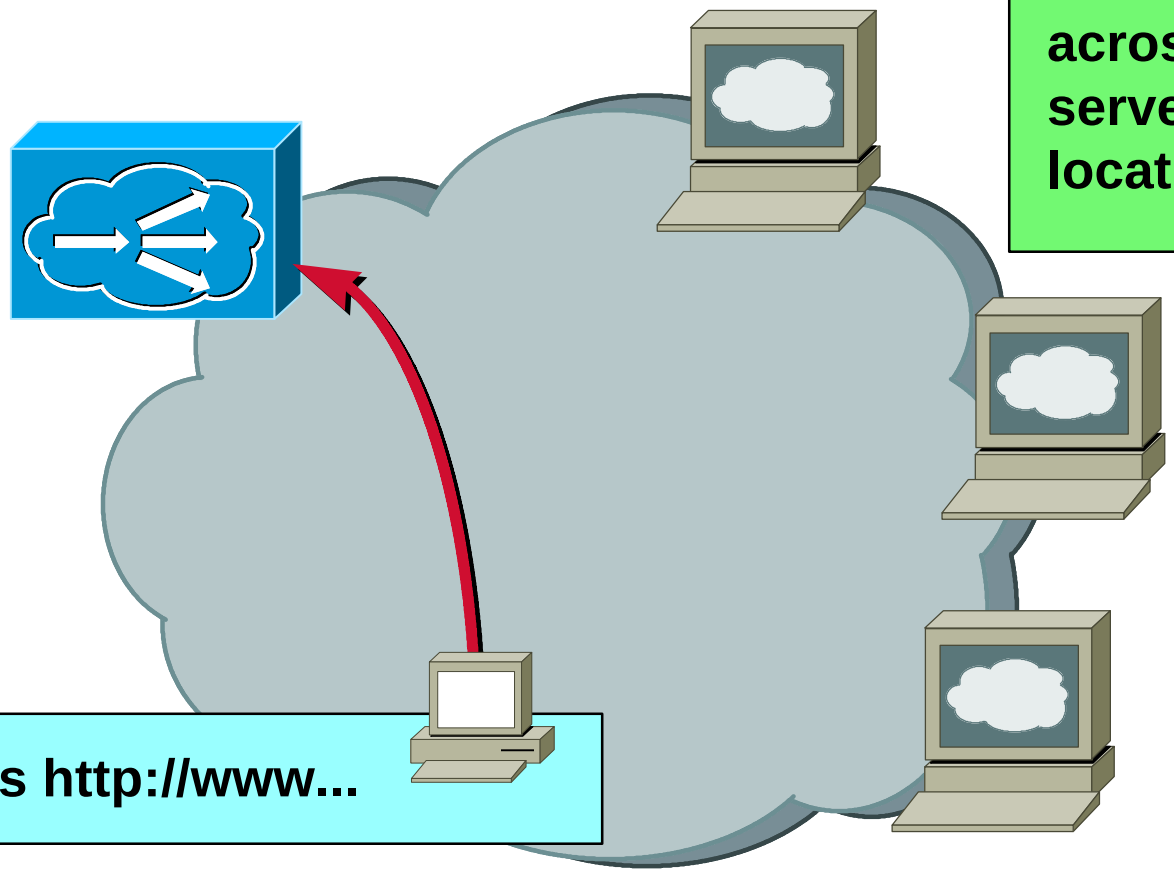
Spread out a vital network service across multiple servers



Cisco Systems

Distributed Director

Spread out a vital network service across multiple servers in diverse locations



Where is http://www...

Cisco Systems

Switch Port Security

```
Console> set port security 3/1 enable 01-02-03-04-05-06
Console> set port security 3/2 enable
Console>
```

```
Console> show port 3
Port  Status   Vlan   Level    Duplex  Speed    Type
----  --------  ----  ------    ------  -----    ------------
3/1   connect  1     normal    half     10      10 BASE-T
3/2   connect  1     normal    half     10      10 BASE-T

Port Security   Secure-Src-Addr  Last-Src-Addr          Shutdown
----  --------  ----------------  -----------------     -------
3/1   enabled   01-02-03-04-05-06  01-02-03-04-05-06     No
3/2   enabled   05-06-07-08-09-10  10-11-12-13-14-15     Yes
Console>
```

CISCO SYSTEMS

Switch Access Security

```
Console> set ip permit 172.100.101.102
Console> set ip permit 172.160.161.0 255.255.192.0
Console> set ip permit enable
```

```
Console> show ip permit
IP permit list feature enabled.
Permit List                Mask
---------------            ---------------
172.100.101.102
172.160.161.0              255.255.192.0
Denied IP Address          Last Accessed Time      Type
-----------------          ----------------        ------
172.100.101.104            01/20/97,07:45:20       SNMP
172.187.206.222            01/21/97,14:23:05       Telnet
Console>
```

CISCO SYSTEMS

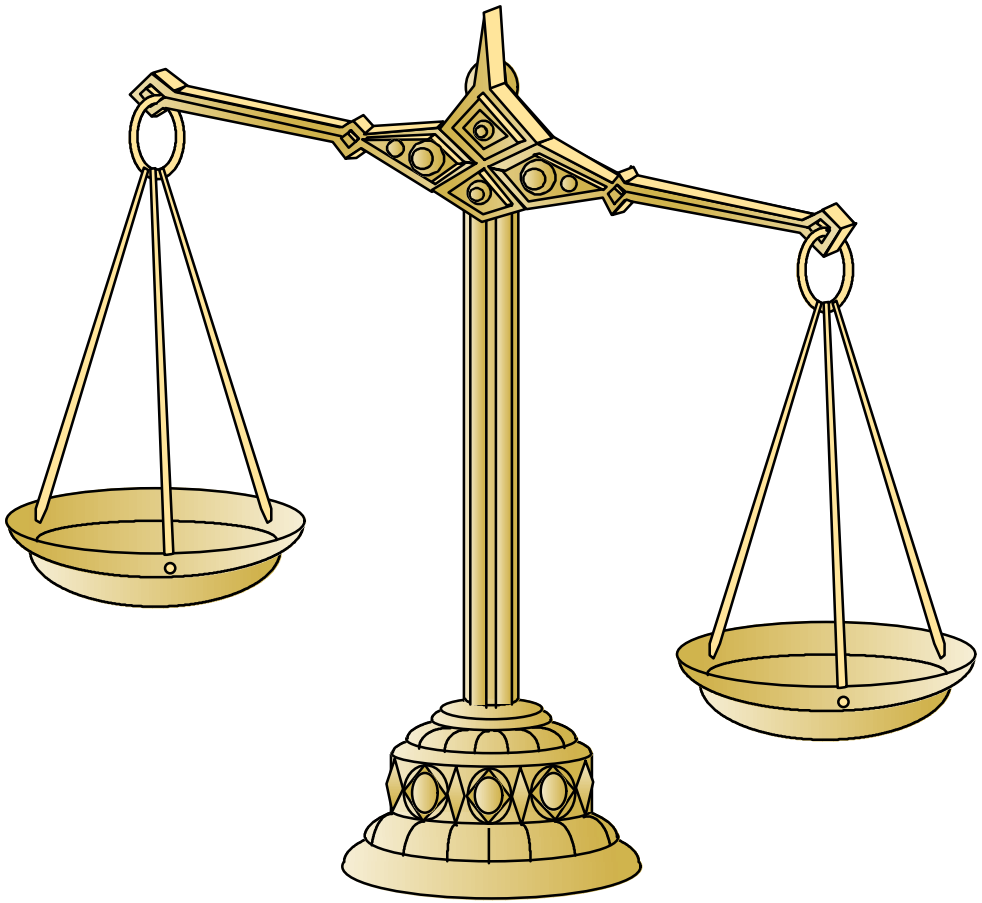
Intranet Protection Costs

- **Versus:**

  Loss

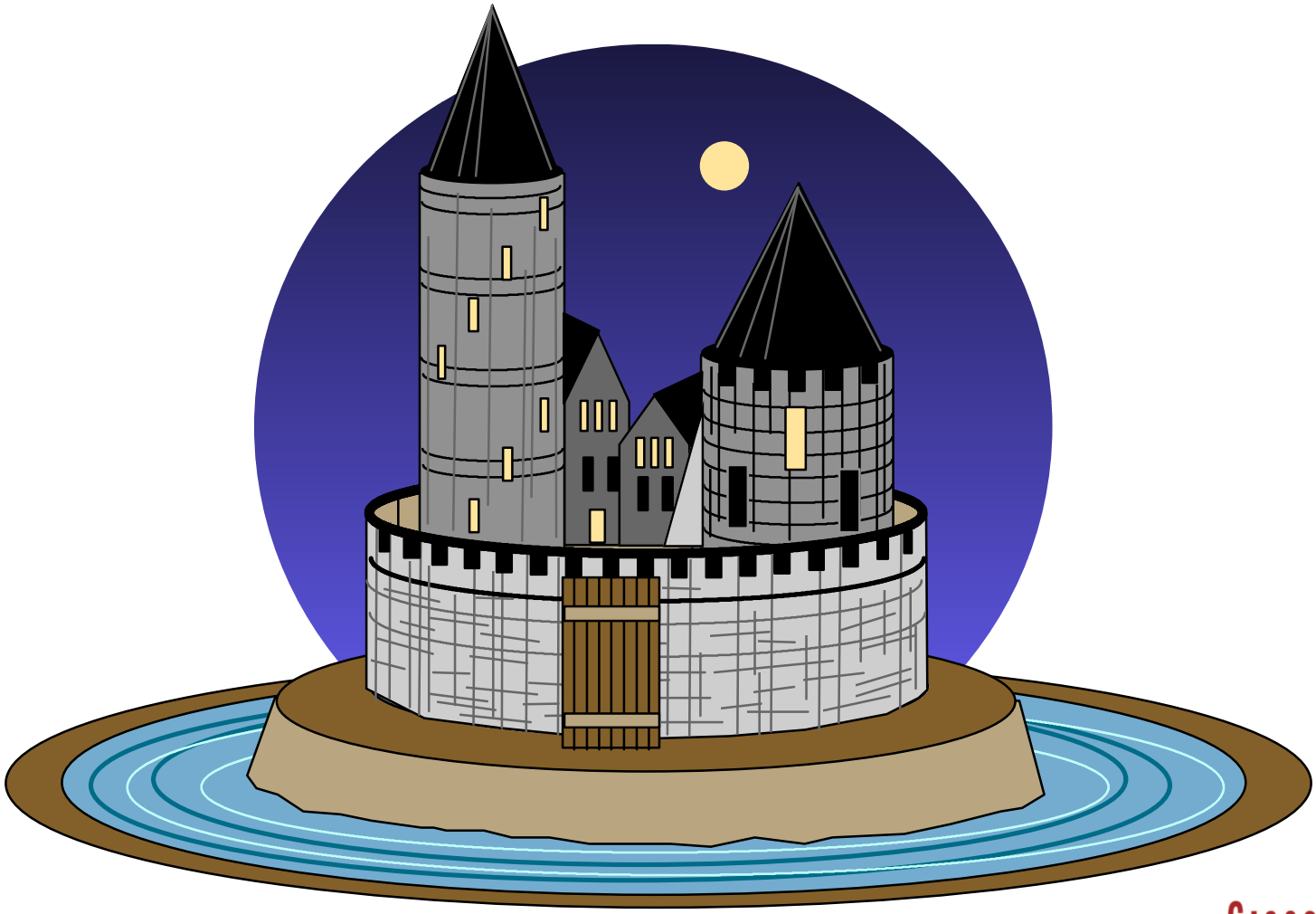
  Corruption

  Ease of Use



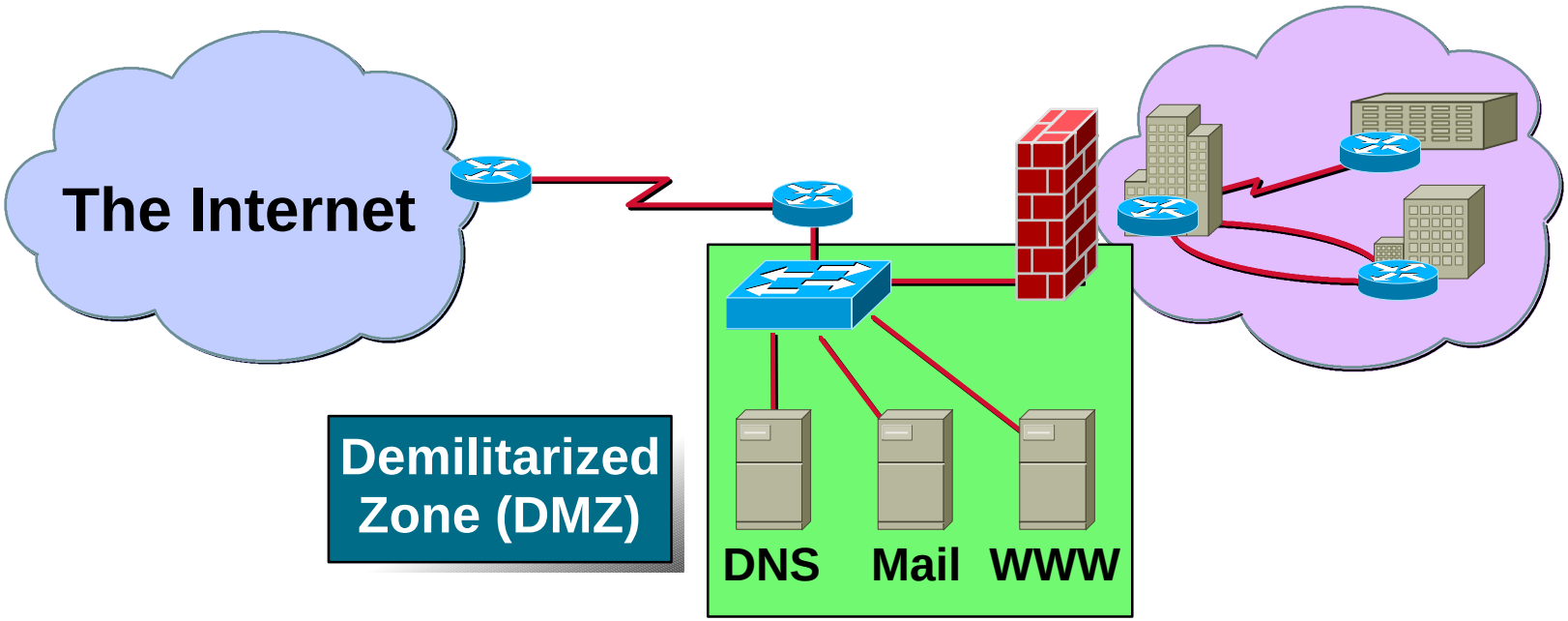
CISCO SYSTEMS

IV. Perimeter Protection



CISCO SYSTEMS

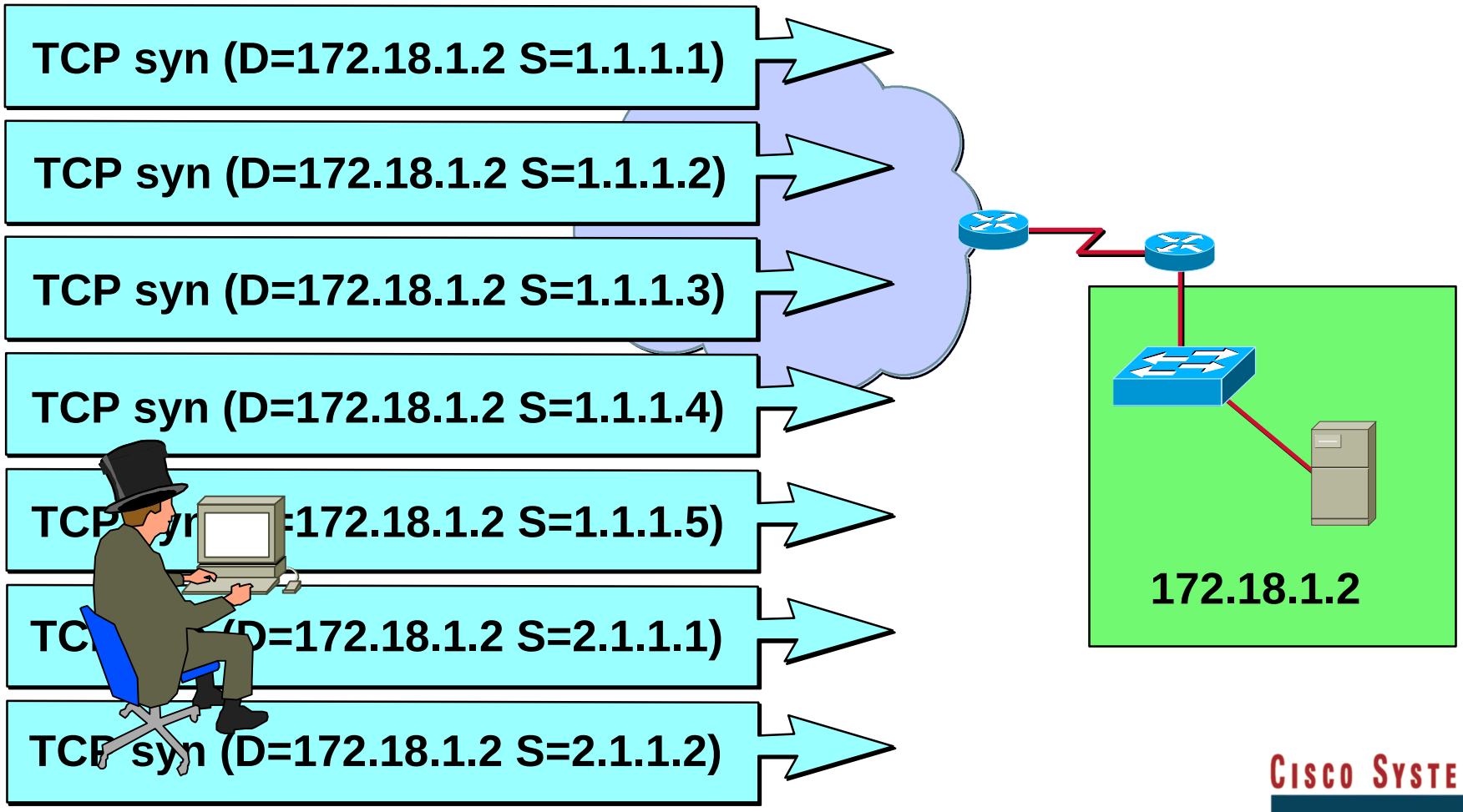
Firewall Protection



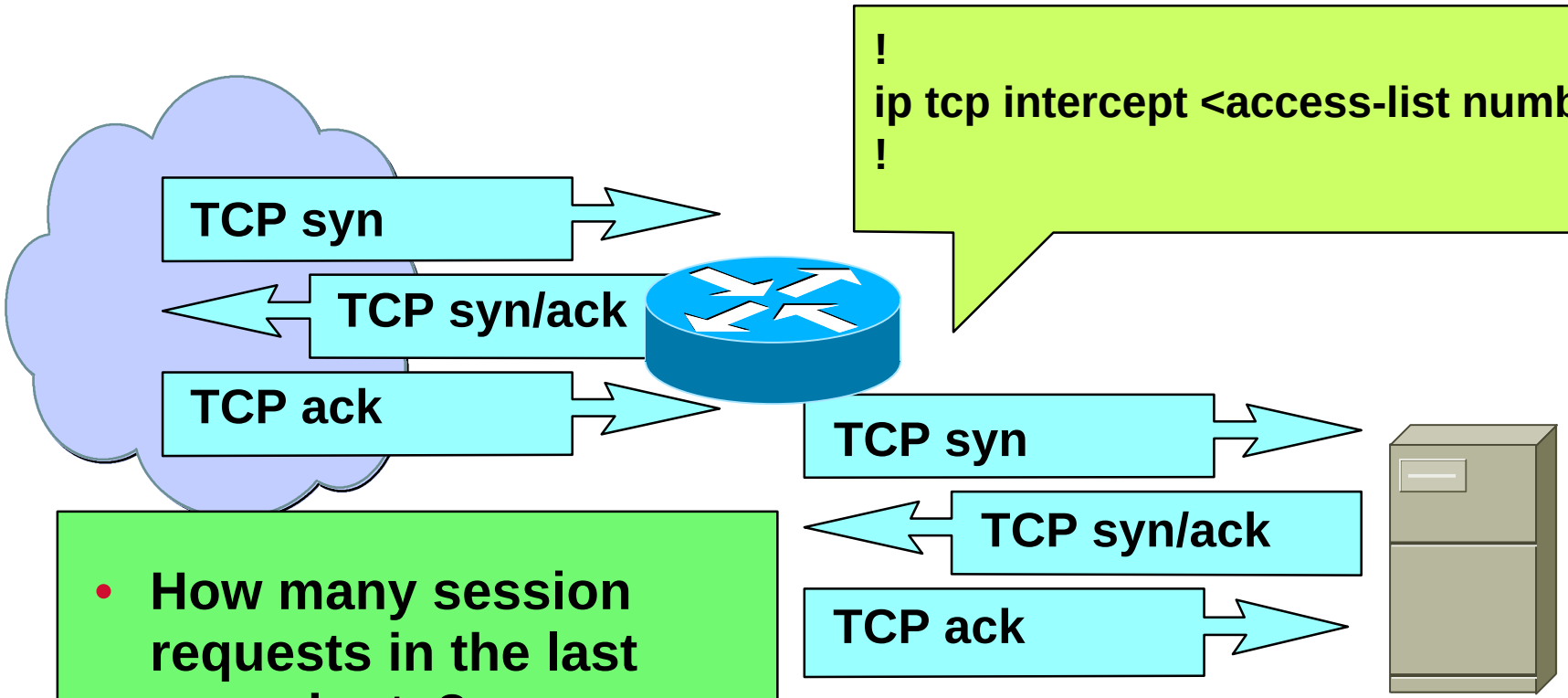
- Use access control lists on the screening router to control traffic
- Isolate each server from traffic with a switch

Cisco Systems

Syn Attack



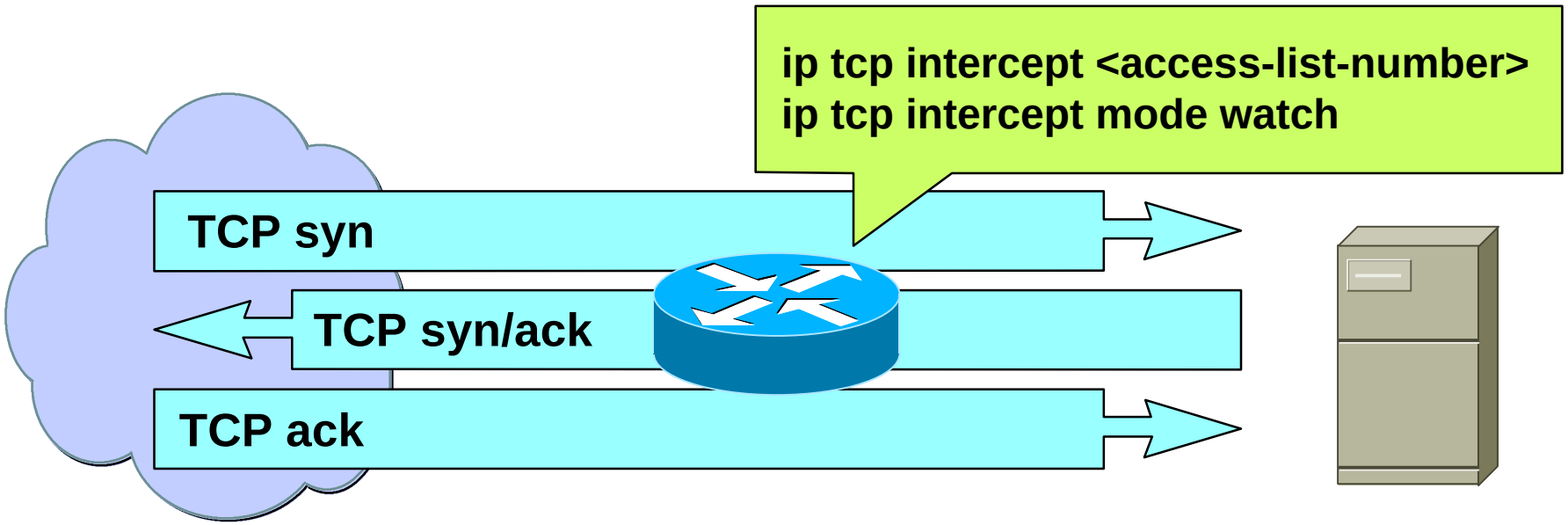
Cisco IOS Syn Attack Defense



- How many session requests in the last one minute?
- How many incomplete sessions are there?

Cisco Systems

Cisco IOS Syn Attack Defense



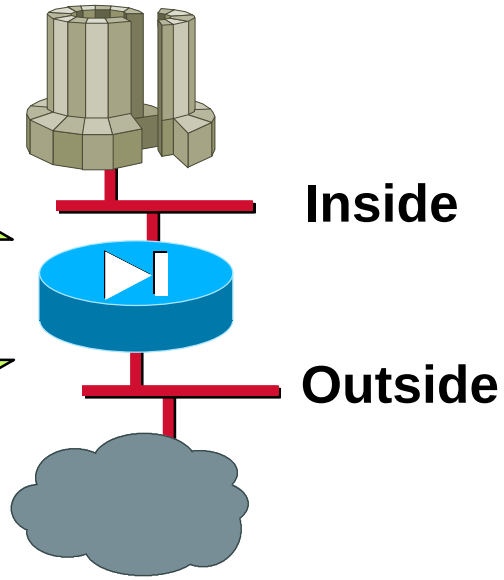
- How many session requests in the last one minute?
- How many incomplete sessions are there?
- How long do I wait for the final ack?

Cisco Systems

PIX—Syn Attack Defense

```
mailhost 172.17.1.12 10.1.1.2 [max_conns] [em_limit]
conduit 172.17.1.12 25 tcp 0.0.0.0  0.0.0.0
```

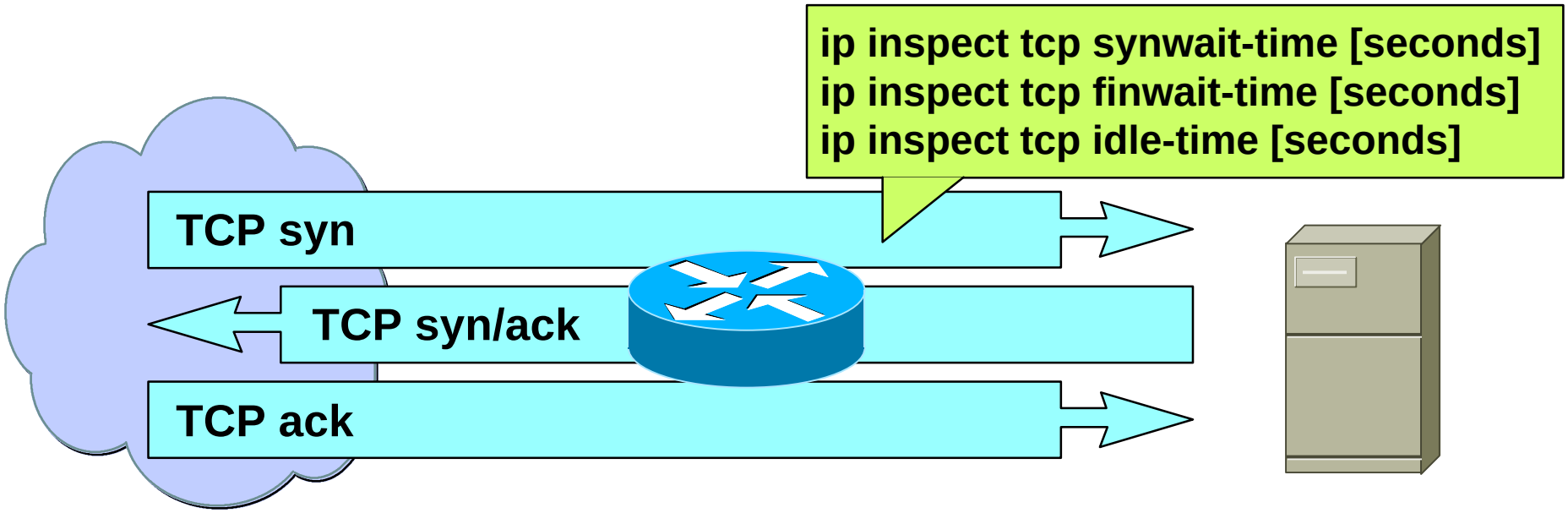
```
static 172.17.1.12 10.1.1.2 [max_conns] [em_limit]
conduit 172.17.1.12 23 tcp 0.0.0.0  0.0.0.0
```



max_conns - the maximum number of TCP connections allowed

em_limit - the embryonic connection limit

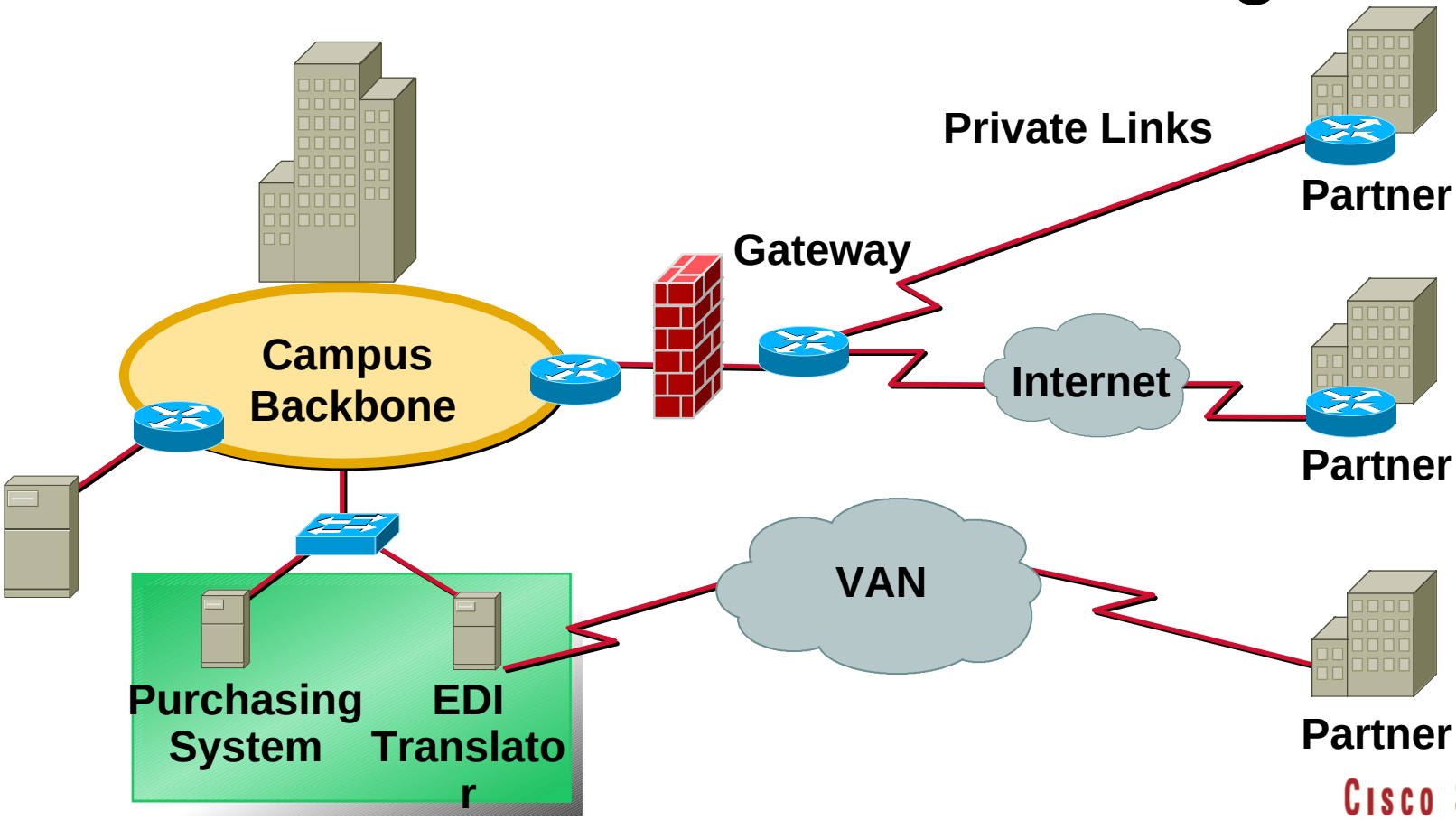
Cisco IOS Firewall Feature Set Syn Attack Defense



- How many session requests in the last one minute?
- How many incomplete sessions are there?
- How long do I wait for the final ack?

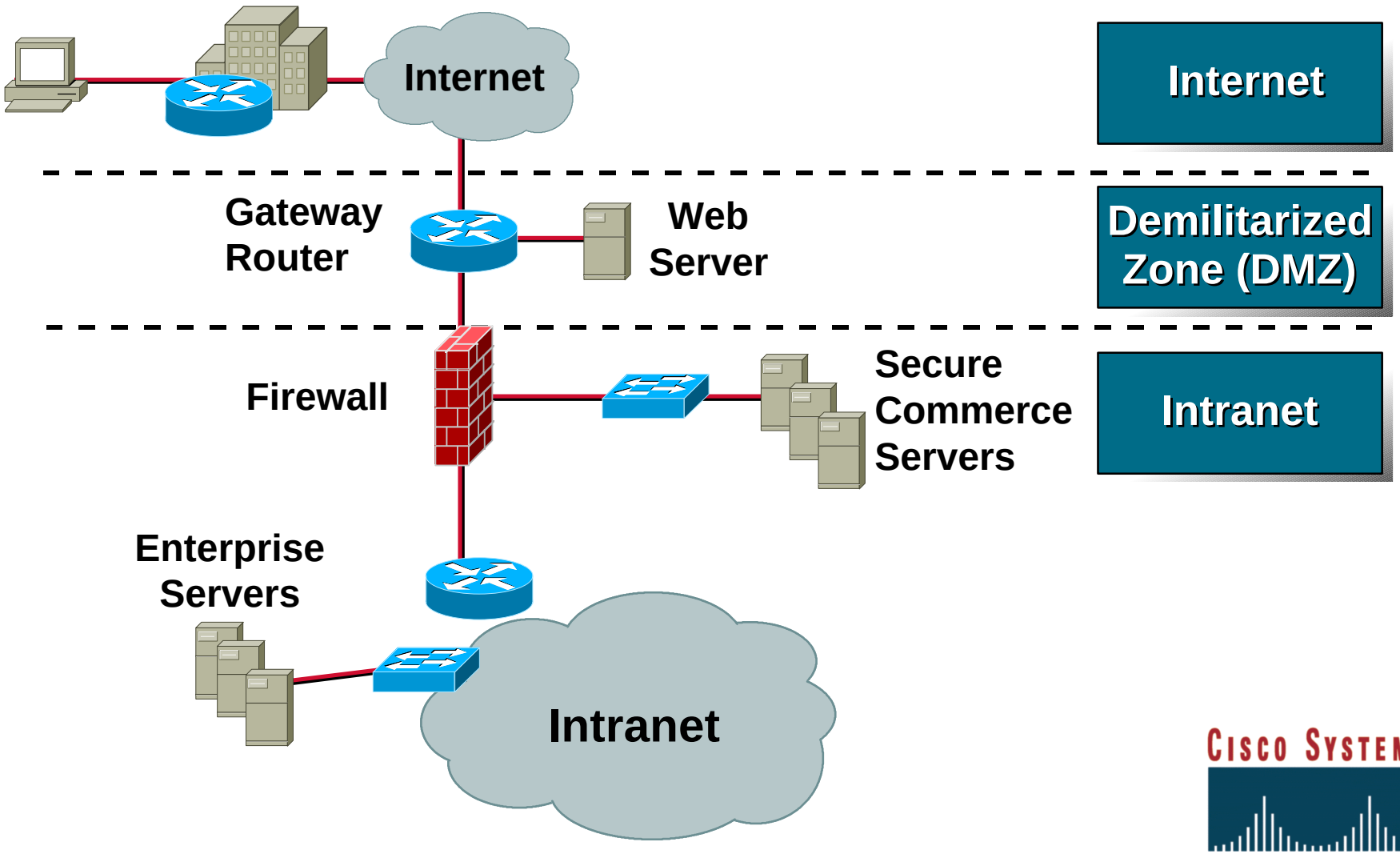
Extranet Options

Virtual Private Networking



Cisco Systems

Electronic Commerce

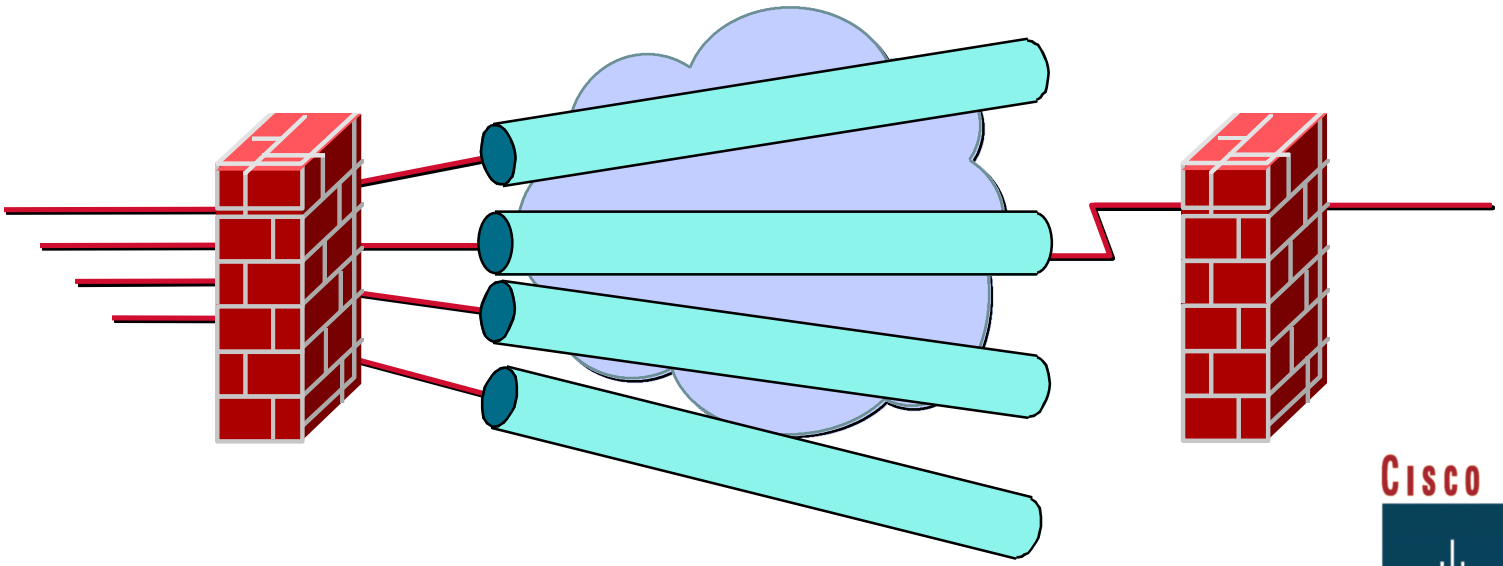


Cisco Systems

VPN Requirements

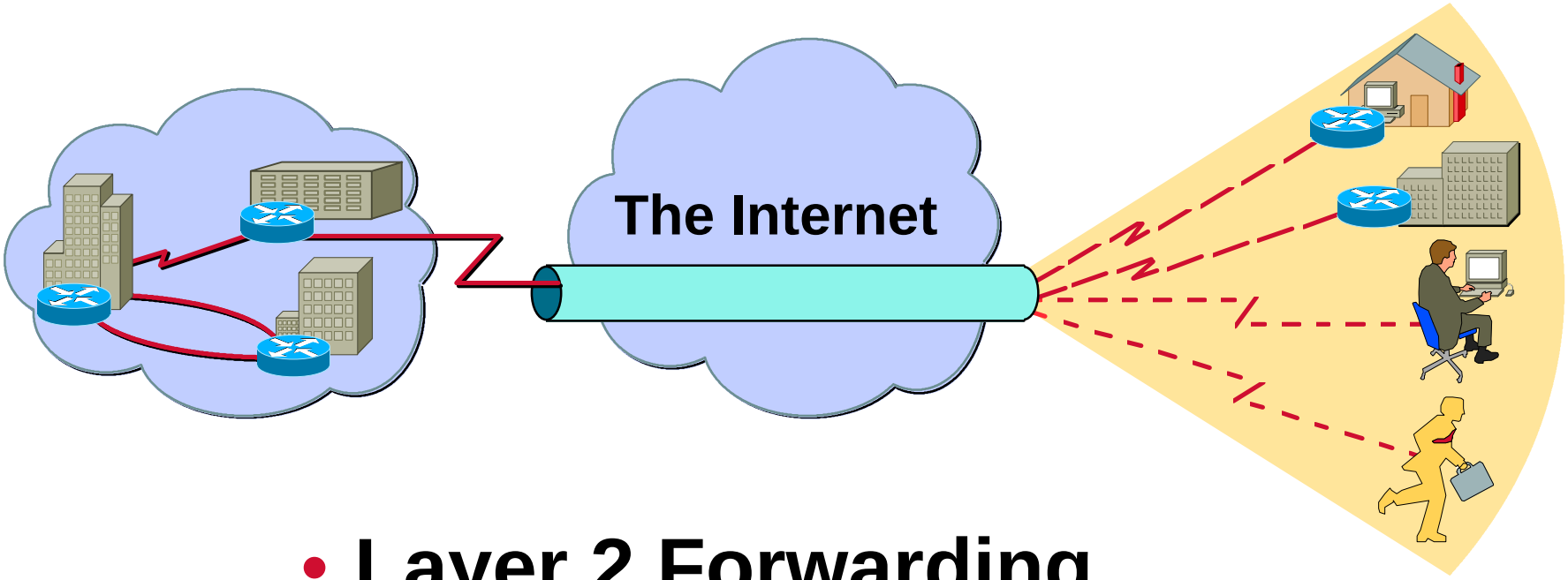
or

- Encryption for authentication, confidentiality and integrity
- Physical line separation via private lines or frame relay



Cisco Systems

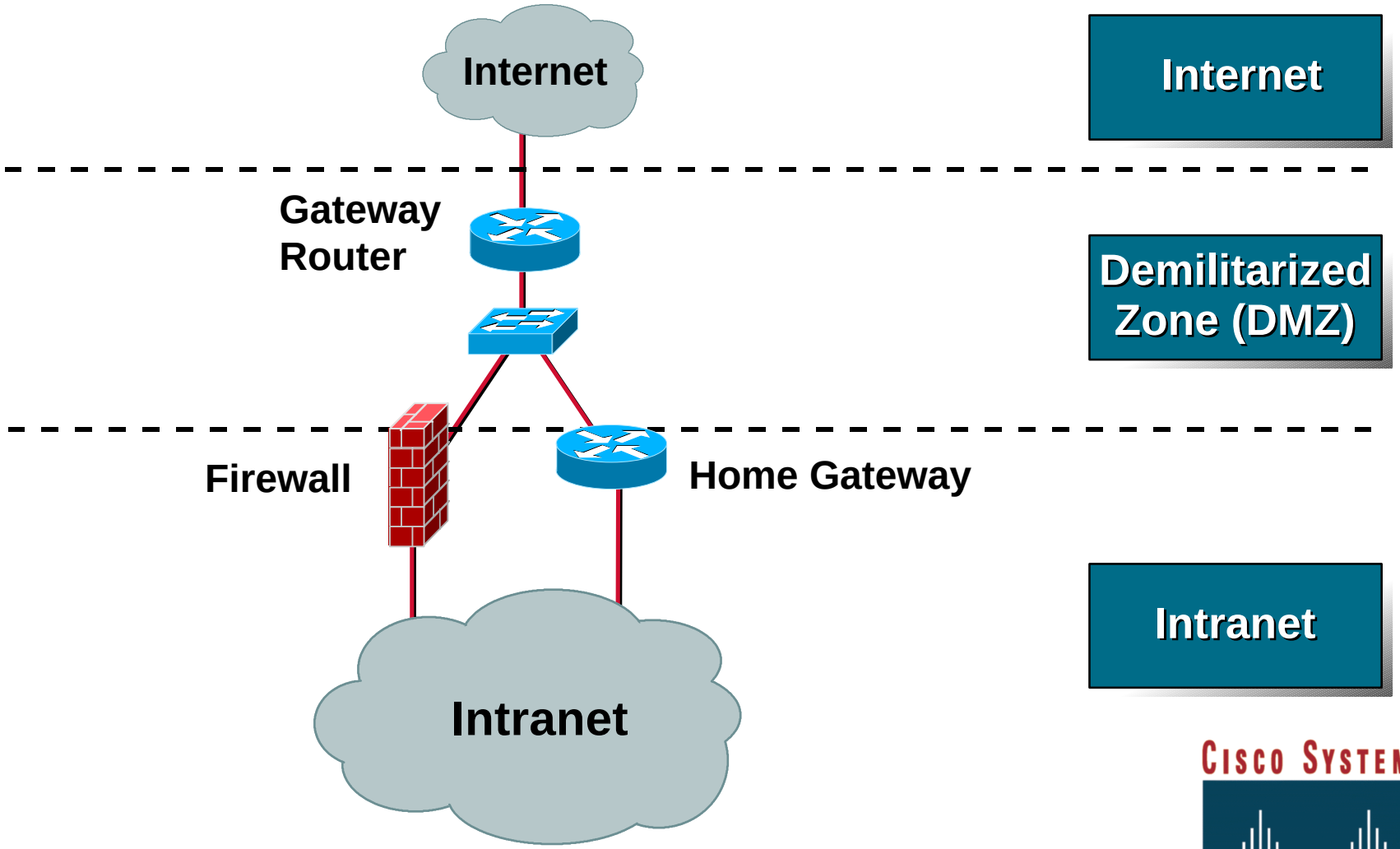
Virtual Private Dial Network



- Layer 2 Forwarding
- Layer 2 Tunnel Protocol

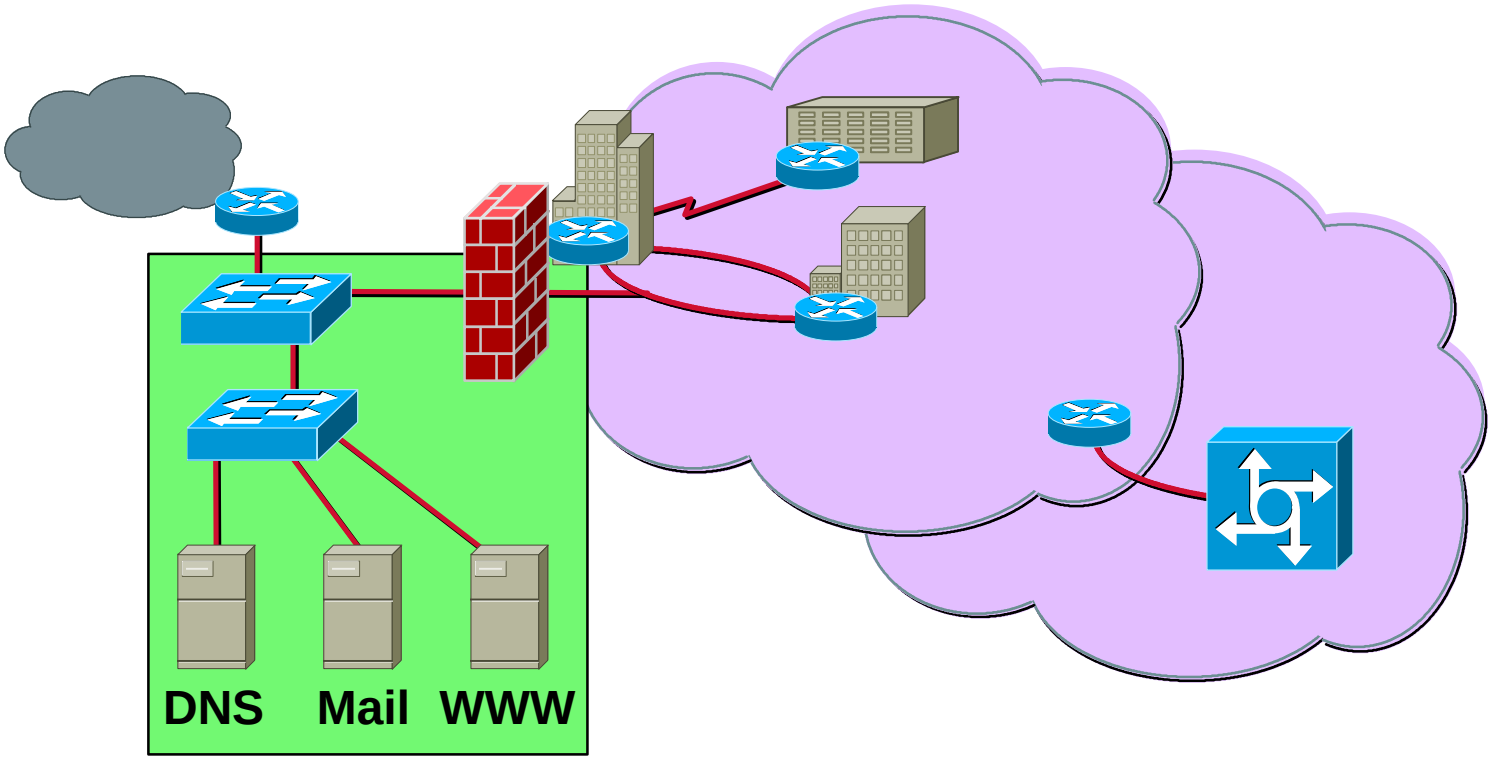
Cisco Systems

VPDN Entrance to the Enterprise



Cisco Systems

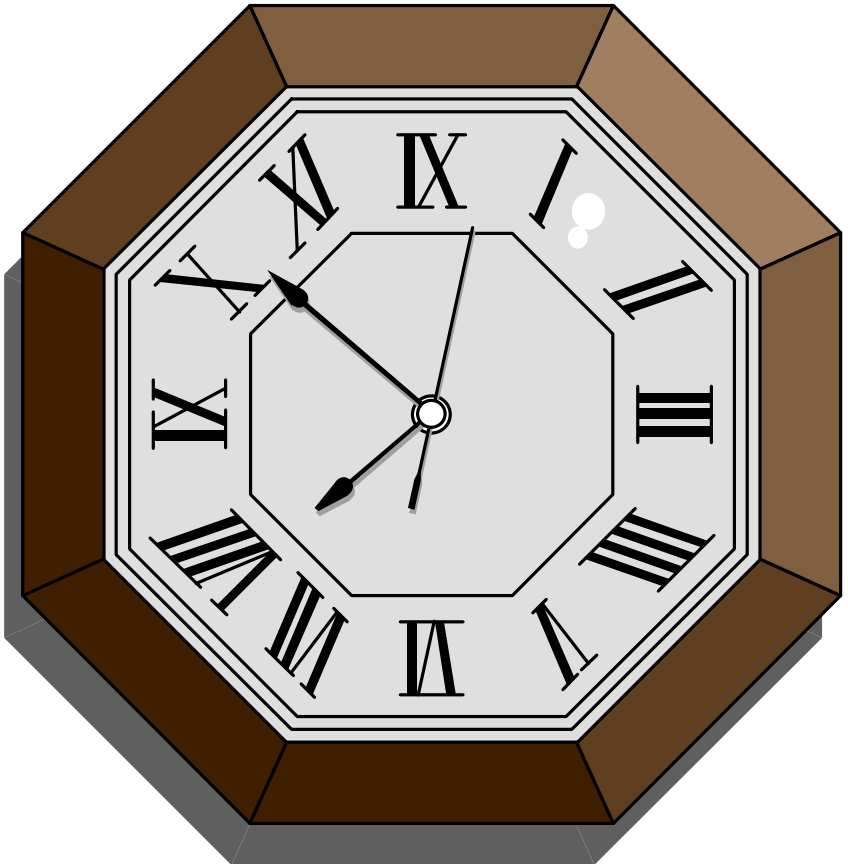
Dial Access Protection



- **Where to place the NAS?**

Cisco Systems

V. Network Security Sustainment

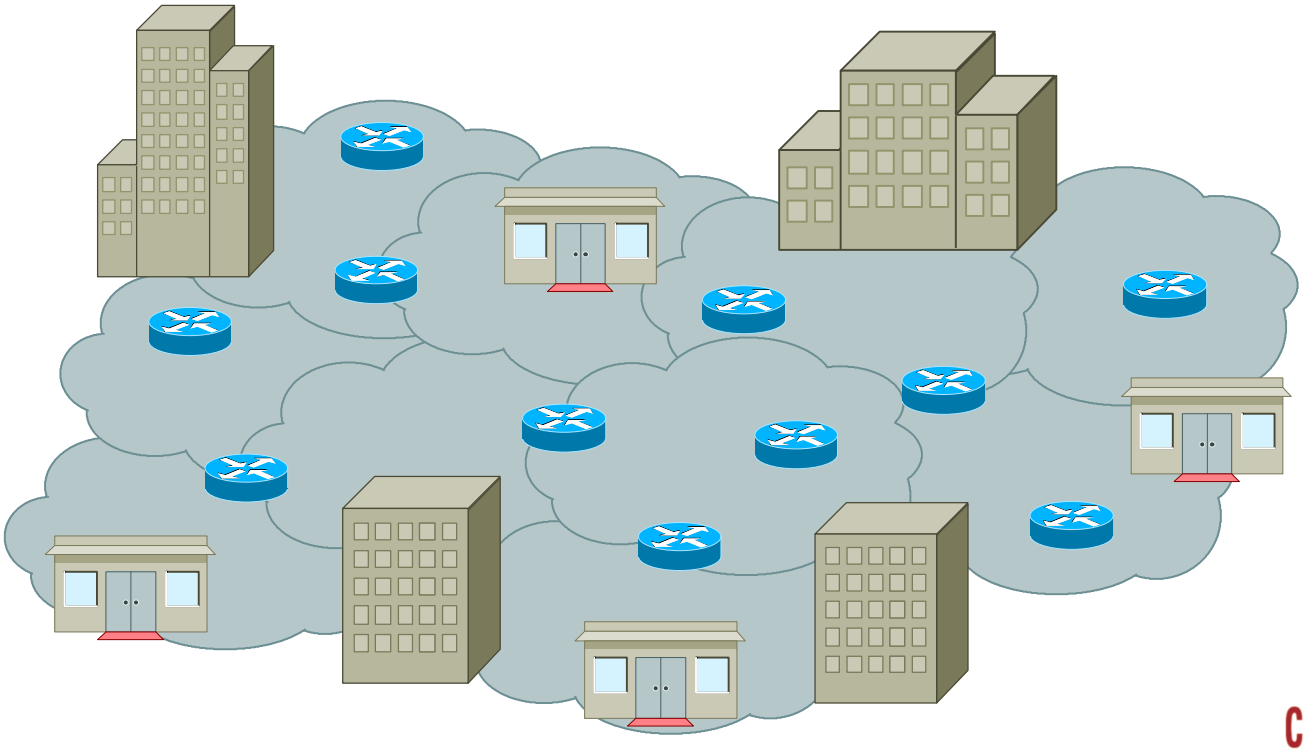


- 24 by 7

CISCO SYSTEMS

Dynamic Routing Protocols

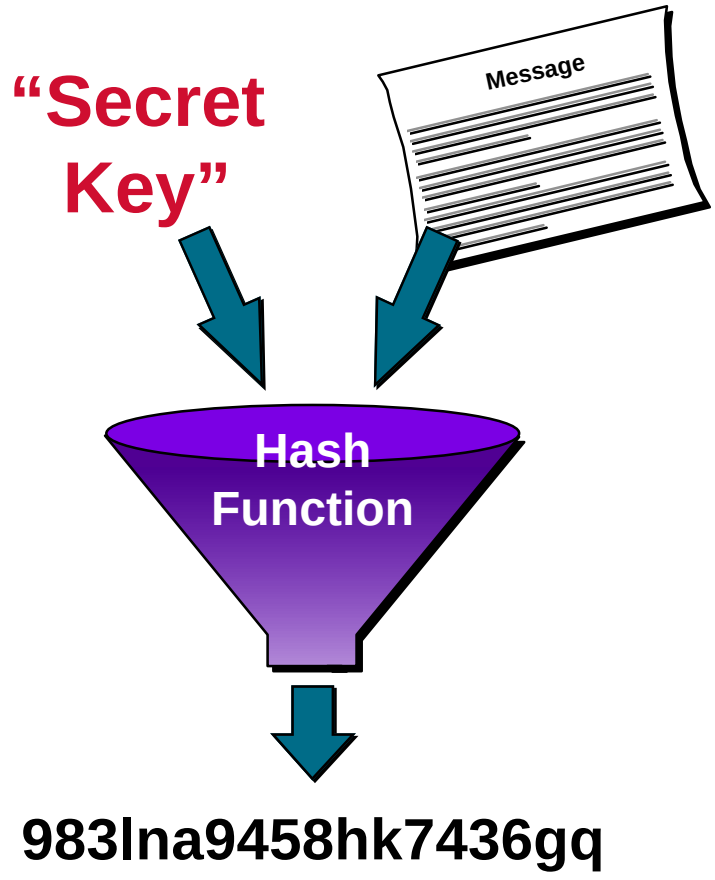
Path Redundancy to Route Around Failures



CISCO SYSTEMS

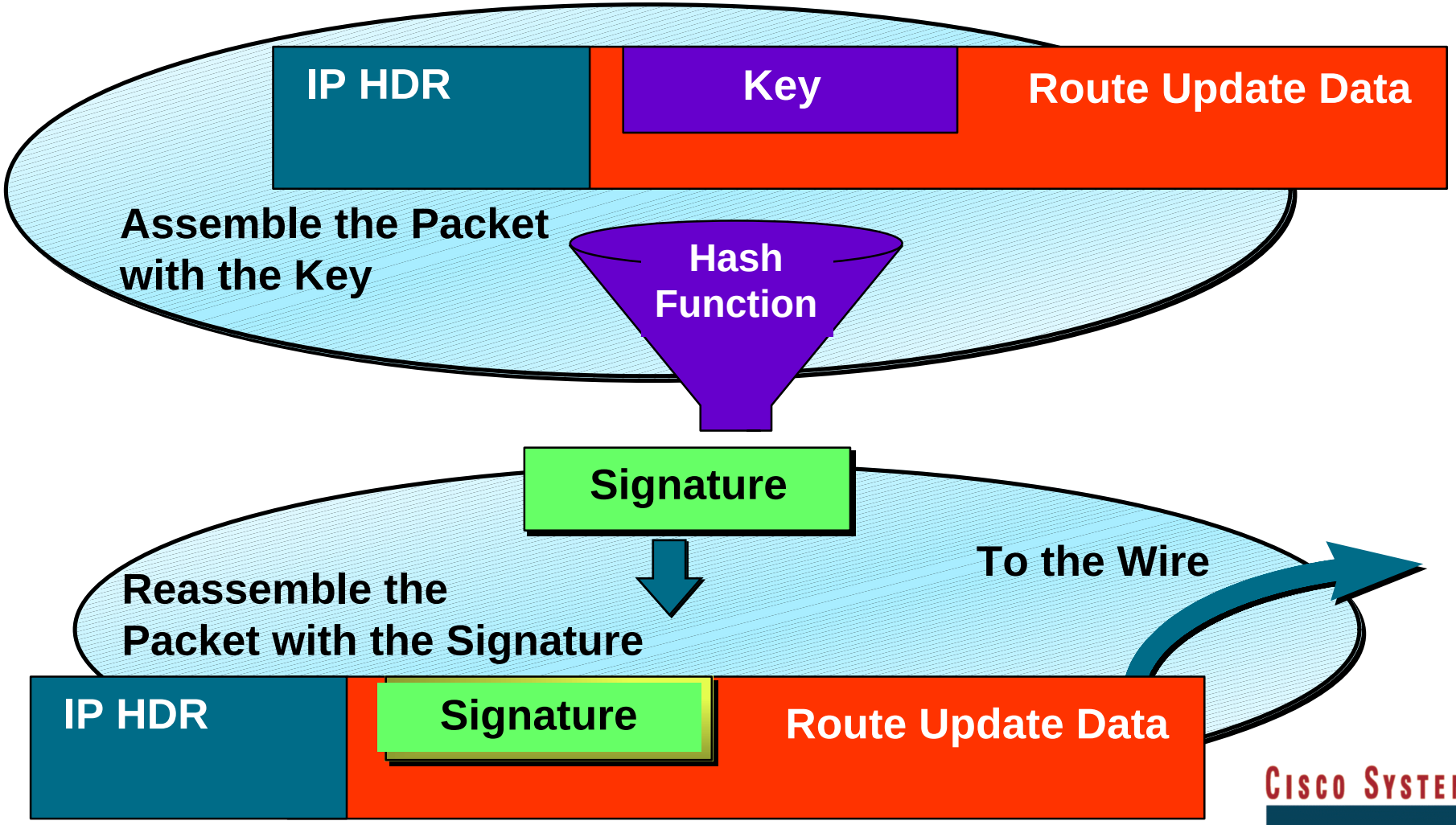
Keyed Hashing for Authentication and Integrity

- Secret key and message are hashed together
- Recomputation of digest verifies that the message originated with the peer and that the message was not altered in transit



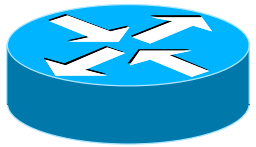
Cisco Systems

Route Update Authentication and Integrity



Route Filtering

```
router rip
 network 10.0.0.0
 distribute-list 1 in
!
access-list 1 deny   0.0.0.0
access-list 1 permit 10.0.0.0  0.255.255.255
```

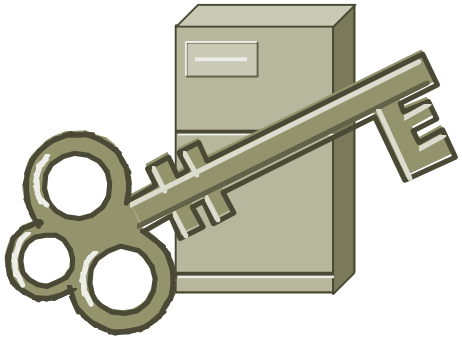


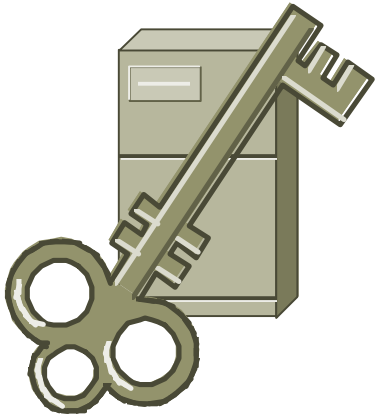
```
Router# sho ip proto
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is 1
  Redistributing: rip
```

CISCO SYSTEMS

Secure Vital Services

- Network Time Protocol Sources
- Domain Name Servers
- Certificate Authority

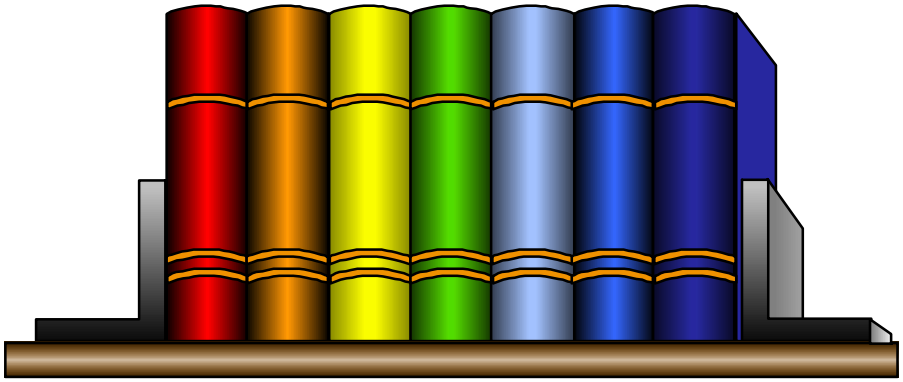




Cisco Systems

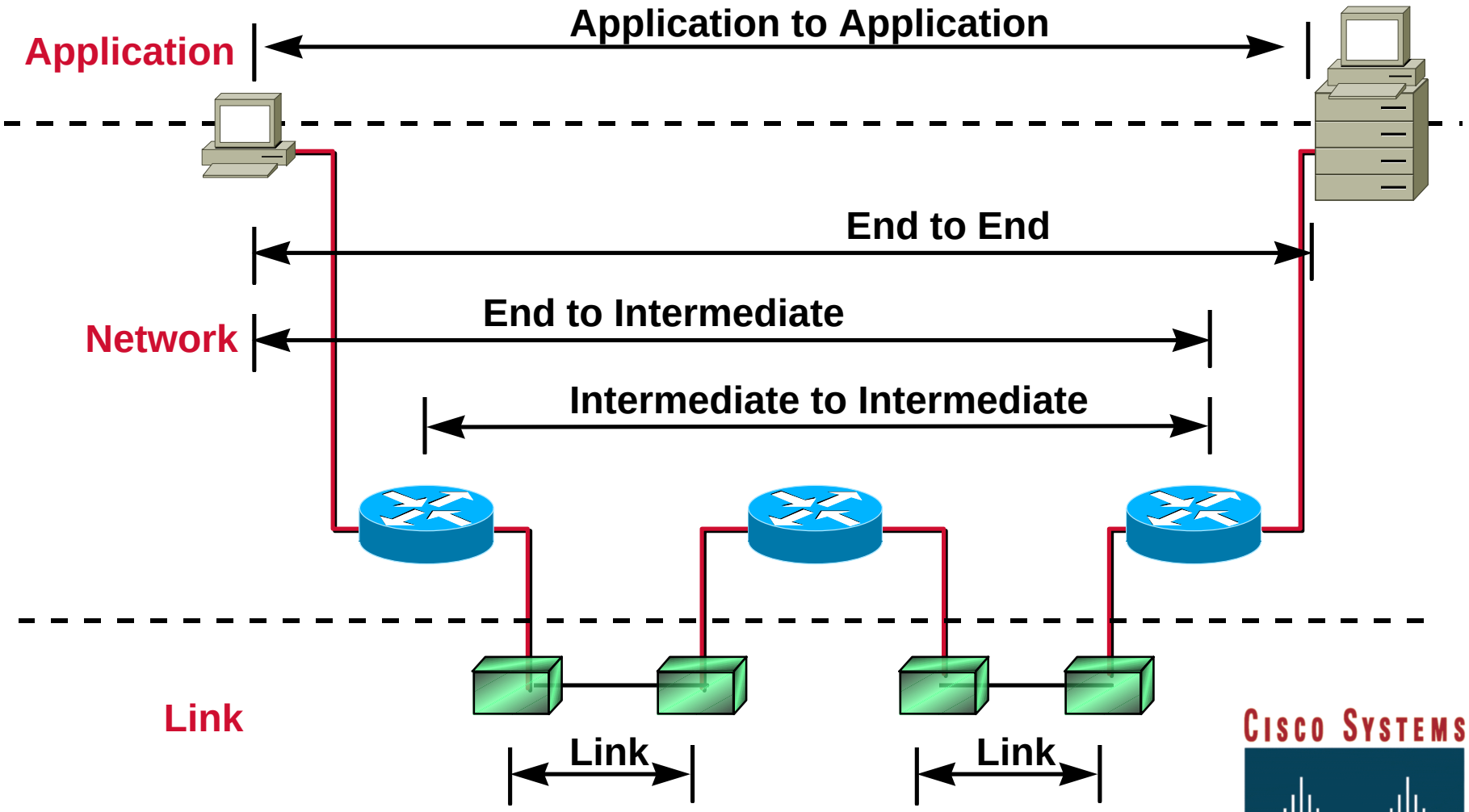
Multi-Level Security (TCSEC)

- Not really needed in Enterprise Networks
- Difficult to implement (unless you're the military)

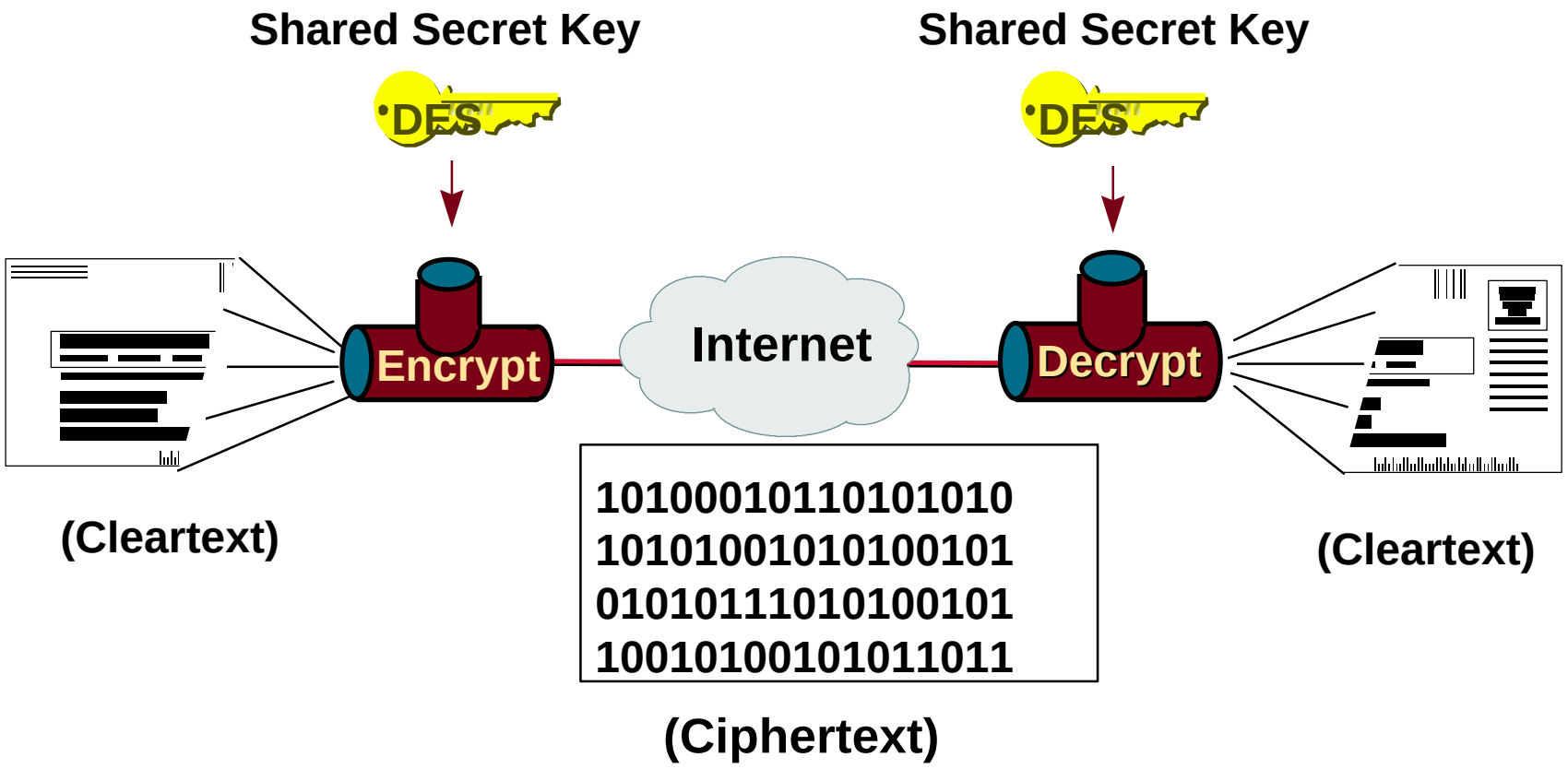


CISCO SYSTEMS

Session Protection through Encryption



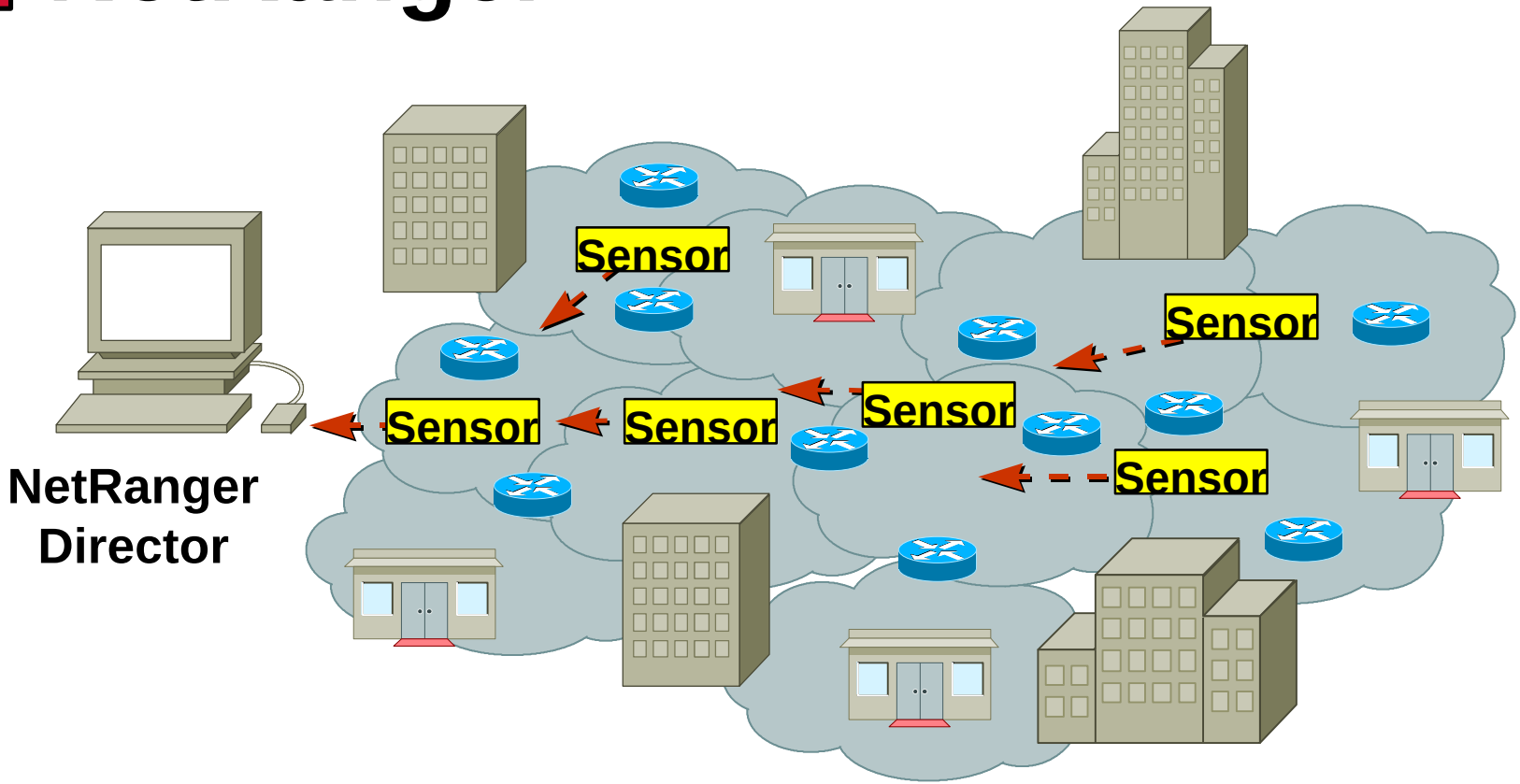
Session Protection through Network Layer Encryption



IPSec—the IETF working group defining IP Security

Cisco Systems

NetRanger

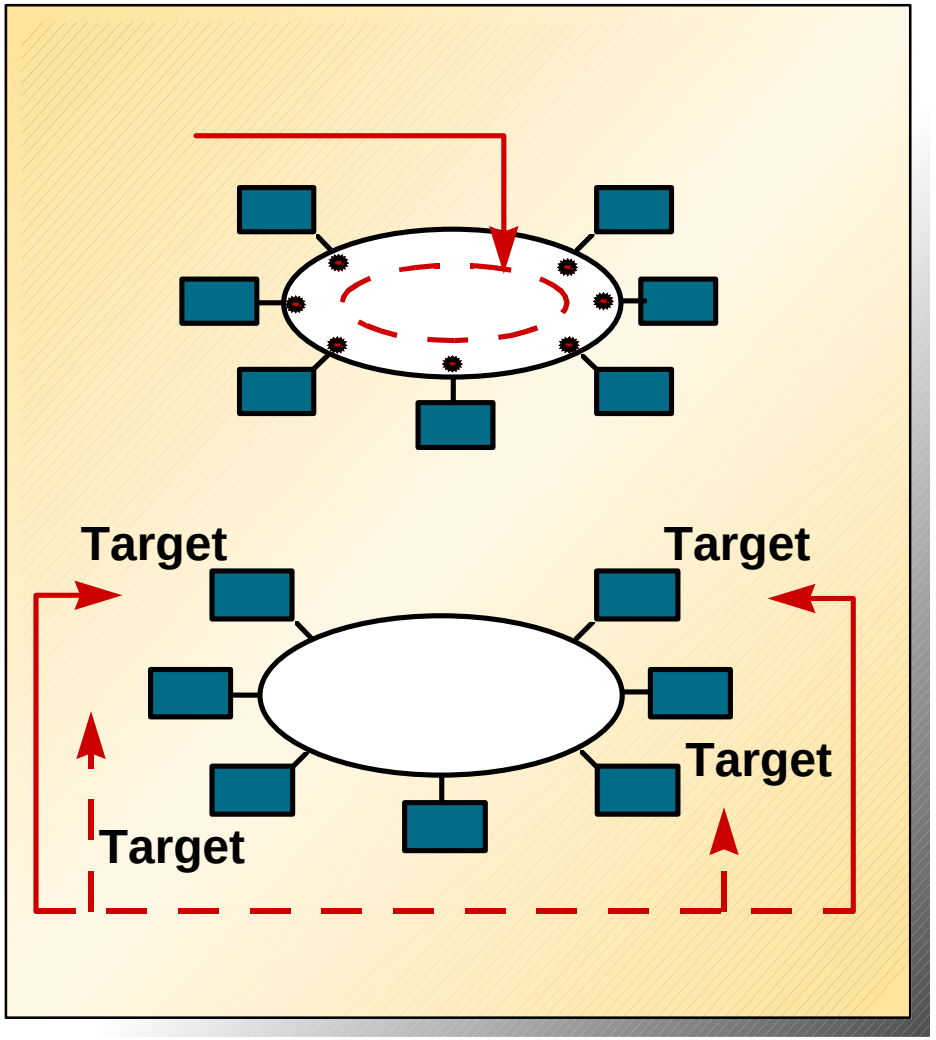


- Sensors watch for attacks or problems
- NetRanger stops active attacks

Cisco Systems

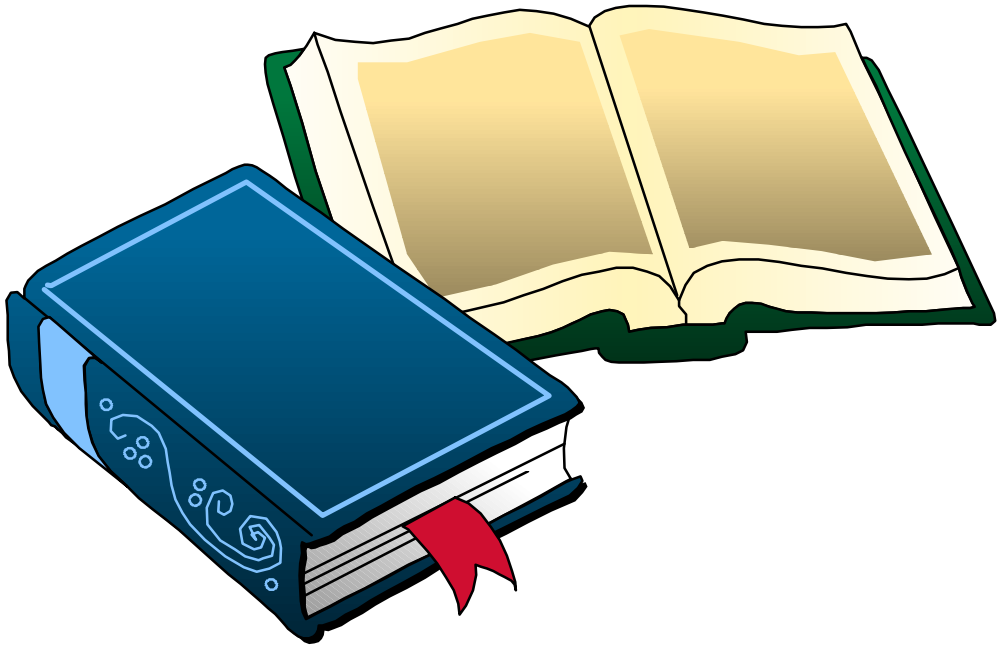
NetSonar Vulnerability Scanning

- **Network mapping**
  - Identify live hosts
  - Identify services on hosts
- **Vulnerability scanning**
  - Analyze discovery data for potential vulnerabilities
  - Confirm vulnerabilities on targeted hosts



VI. Security Sustainment Validation

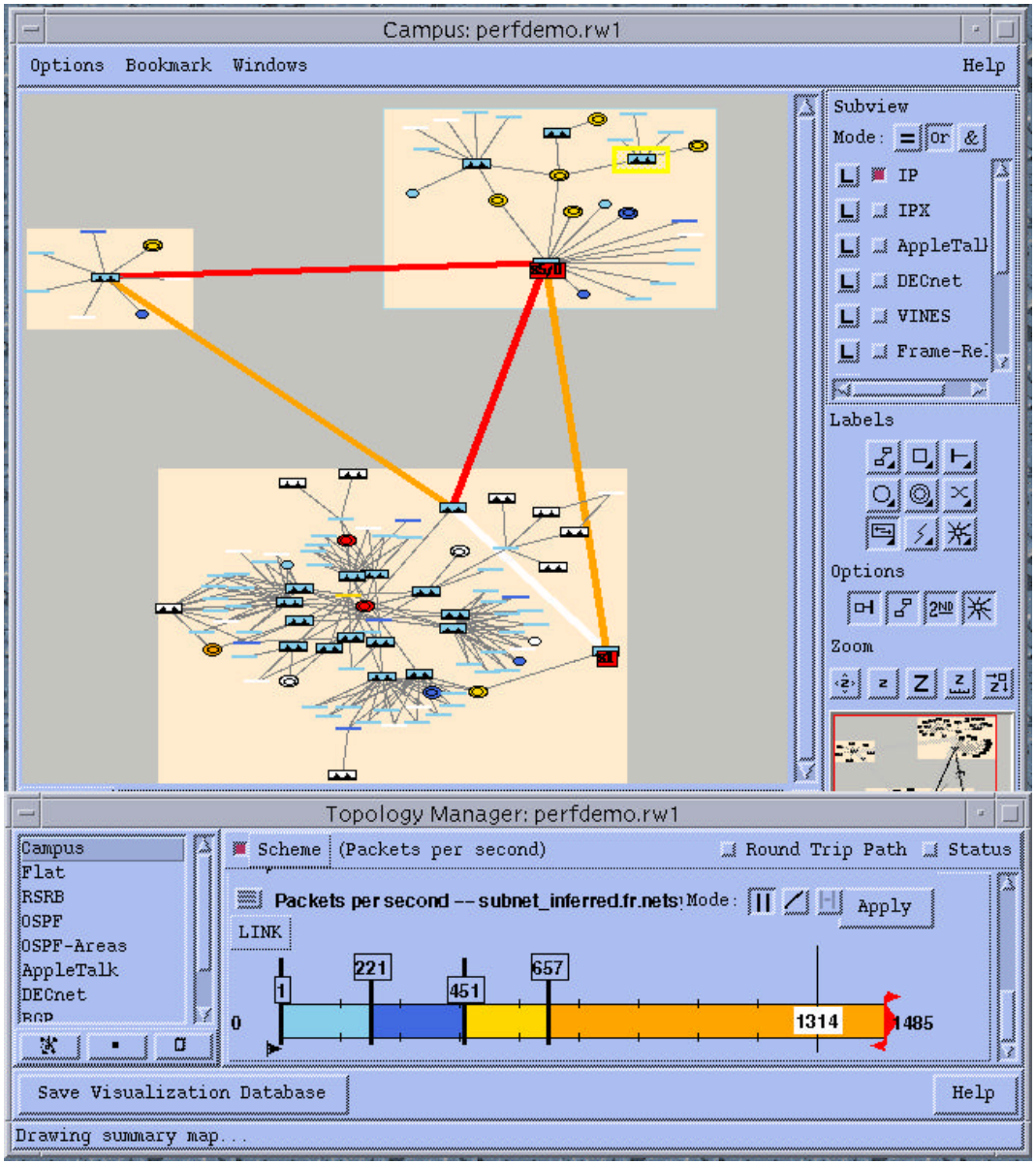
What steps can you take to make sure that your network will continue to be secure?



Cisco Systems

Modeling Tools

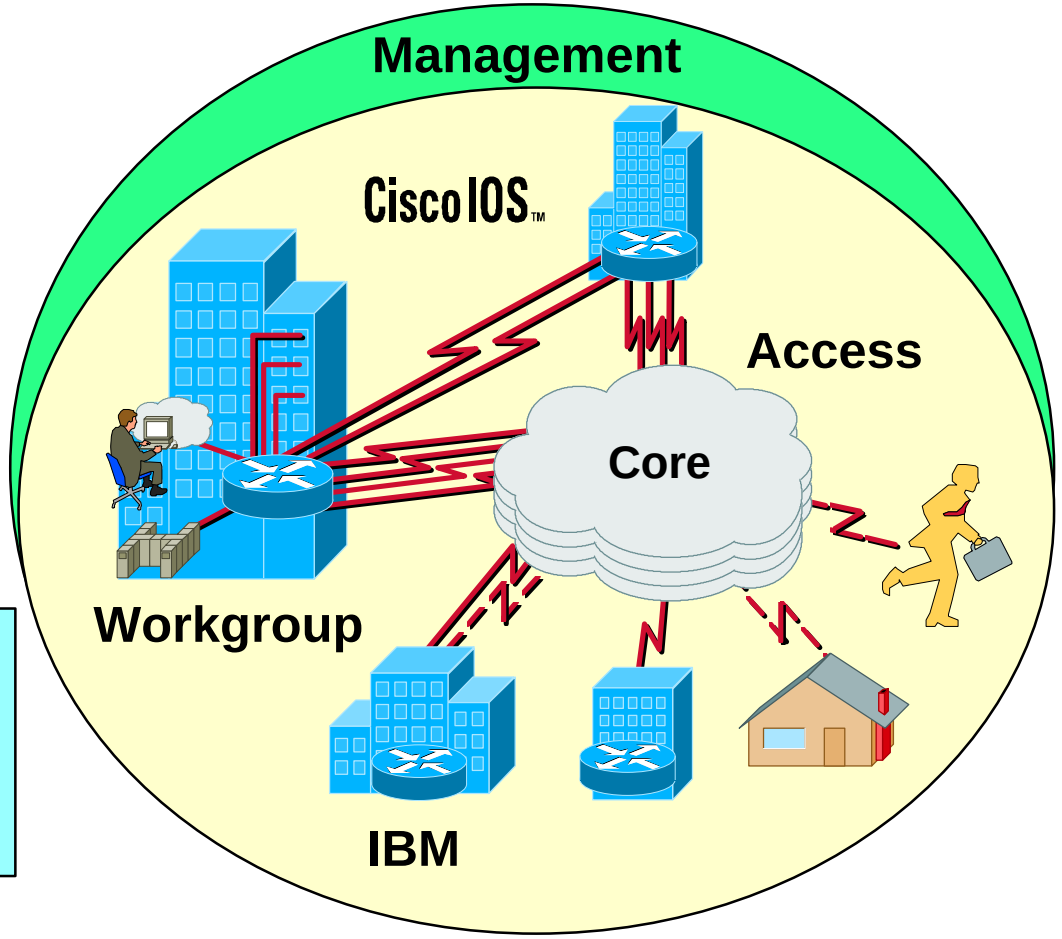
- **NetSys Modeling can verify the access controls in your network**



Validating Your Policy through Network Management Systems

- What to monitor?
- What to measure?

Track and report trends that show how you are achieving your security goals



VII. Conclusions

For the want of a nail, the shoe was lost.

For the want of a shoe, the horse was lost.

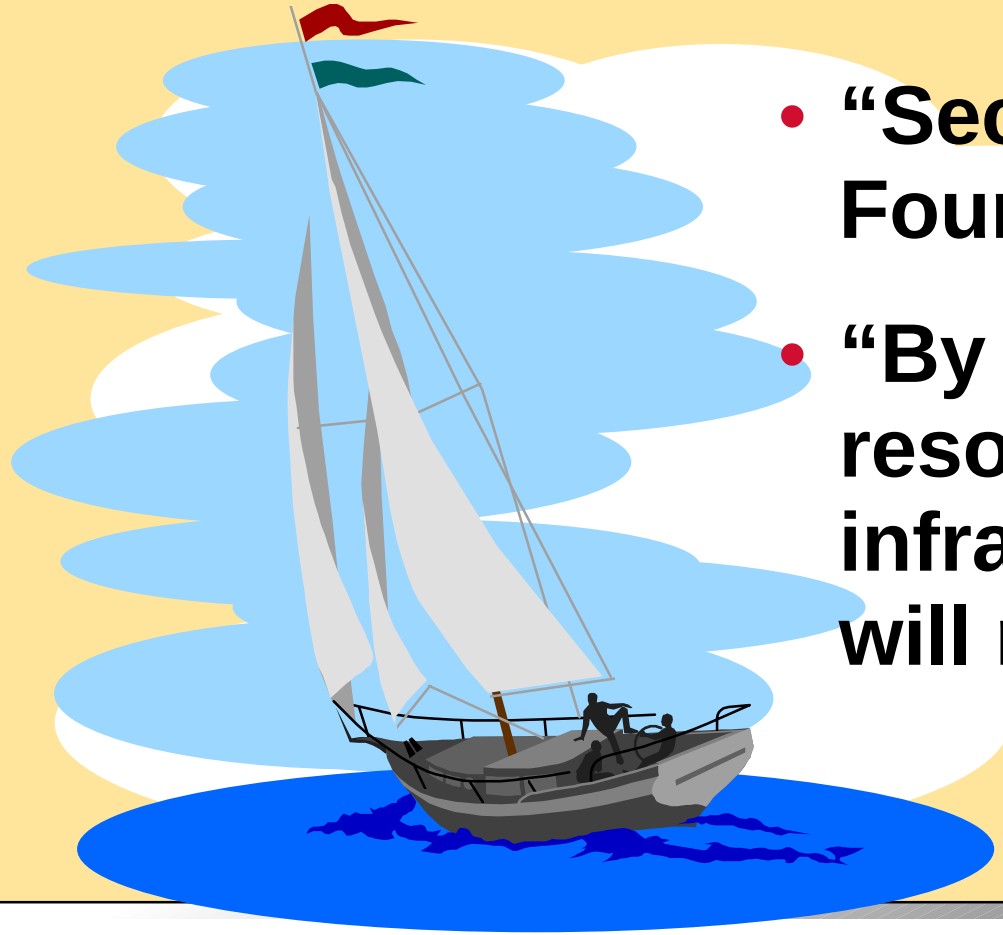
For the want of a horse, the rider was lost.

For the want of a rider, the battle was lost.

For the want of a battle, the Kingdom was lost.

And all for the want of a horse shoe nail.

Smooth Sailing



- “Security is a Foundation Service”
- “By protecting the resources and the infrastructure, things will run properly”

Cisco Systems


CISCO SYSTEMS
EMPOWERING THE
INTERNET GENERATION℠