IPv6 Business Information Exchange

Nalini Elkins
Inside Products, Inc.
April 21, 2009
(831) 659-8360

Inside Products, Inc.
www.insidethestack.com
866-547-9593
sales@insidethestack.com

IPv6 Firewall

Eric Vyncke
Distinguished Engineer
evyncke@cisco.com

Agenda

- Differences between IPv4 and IPv6 firewall
- How to enforce an IPv6 security policy?
- Cisco products
- Conclusion

The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...

  Interesting **scalability** issue (n^2 issue with IPsec)

  Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall

    IOS 12.4(20)T can parse the AH

  Network **telemetry is blinded**: NetFlow of little use

  Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets.

ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

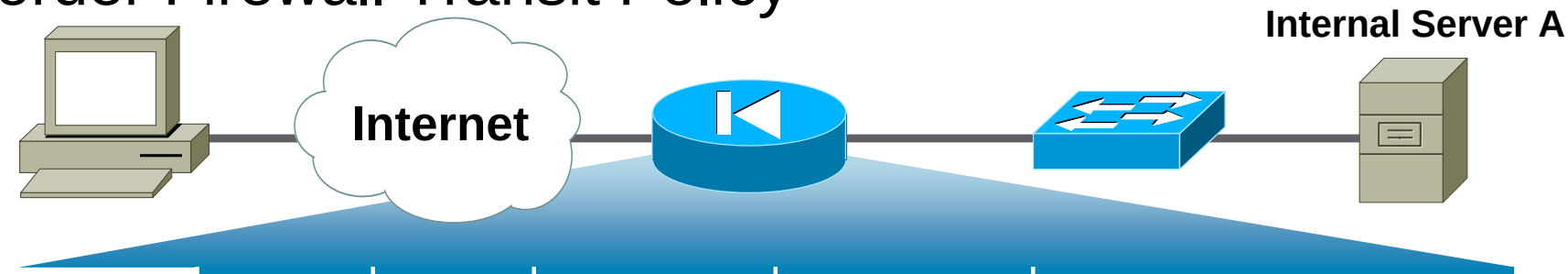
ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

Equivalent ICMPv6

For Your Reference

Border Firewall Transit Policy*

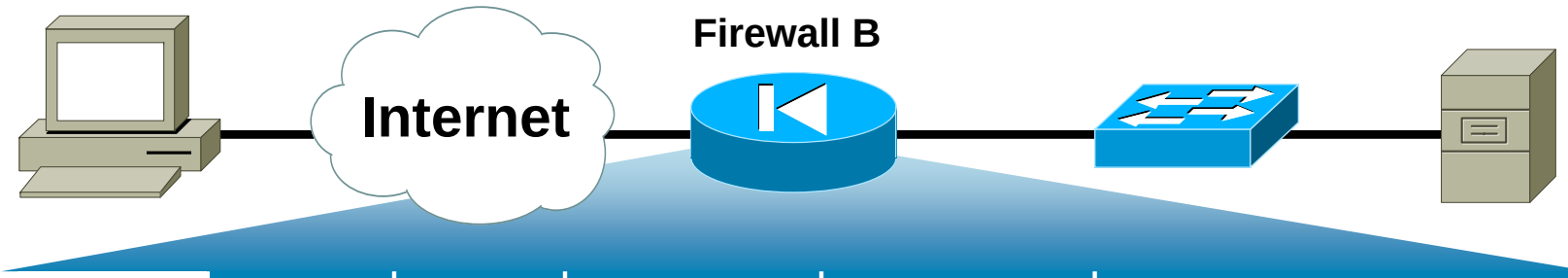


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded
Permit	Any	A	4	0	Parameter Problem

*RFC 4890

Potential Additional ICMPv6

Border Firewall Receive Policy*



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	133/134	0	Neighbor Solicitation and Advertisement
Permit	Any	B	4	0	Parameter Problem

*RFC 4890

Application Inspection Engines

- Stateful-inspection firewall must also update their application support:

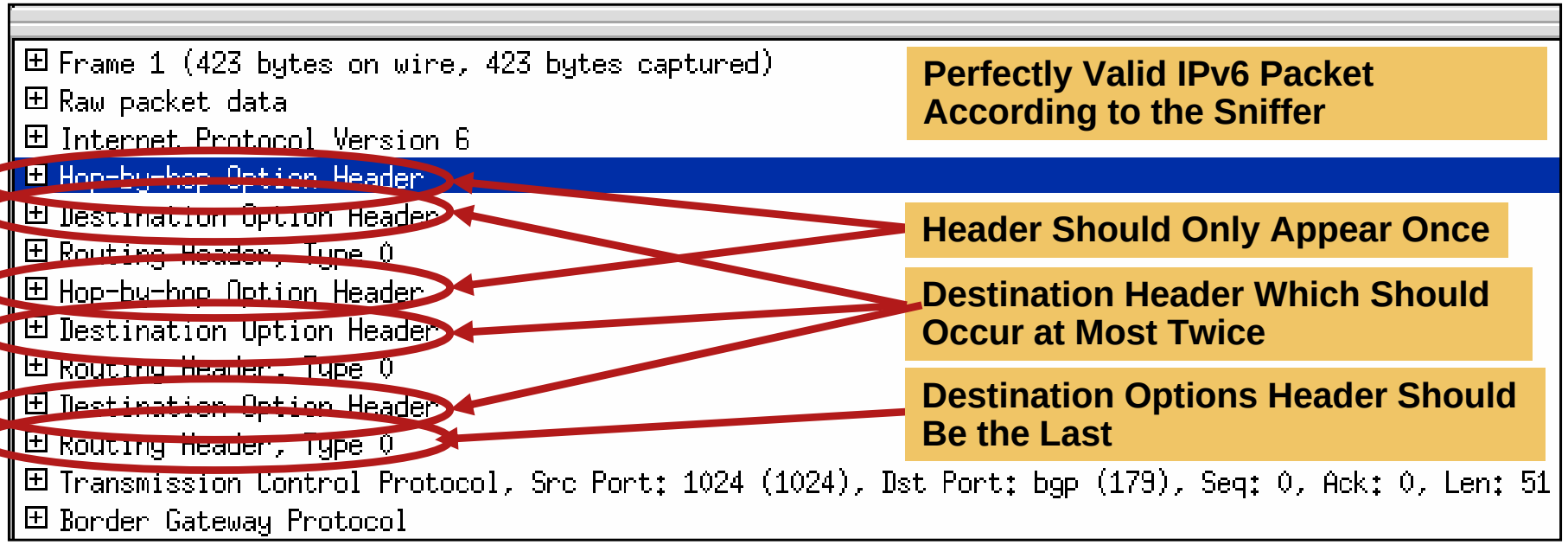
  ICMPv6: different syntax and slightly different semantics

  FTP: RFC 2428 replace PASV with EPSV, ...

  HTTP, SMTP, SIP, ...: no real changes

IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?



IPv6 Extension Header Parsing

- Firewalls (like hosts) need to parse Extension Headers to find TCP/UDP information
- Procedure to find L4 protocol information
  1. Parse known Next Header until the L4 header or unknown NH
  2. Check if enough of the L4 protocol header is within the first fragment
- Notes:

⇒ AH can also be skipped

⇒ if chain is too long on HW routers, packet is process switched...

Enforcing an IPv6 Security Policy

- Important:

  In a dual-stack environment, security policies for IPv4 and IPv6 MUST BE identical

  Else, the miscreant will use the less protected protocol

  Also, easier for operation and incident handling

- This also applies to topology (identical perimeter)

  Except, may be, dedicated IPv4 and dedicated IPv6 firewalls (to increase software stability)

PCI DSS Compliance and IPv6

- Payment Card Industry Data Security Standard requires the use of NAT for security

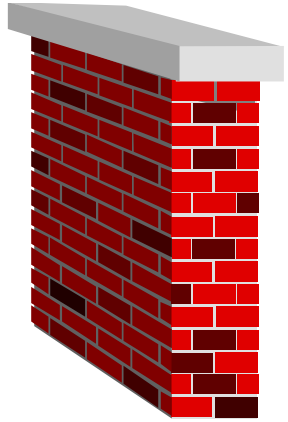
  Yes, weird isn't it?

  There is no NAT IPv6 <-> IPv6 in most of the firewalls

    IETF has just started to work on NAT66

- ➔ PCI DSS compliance cannot be achieved for IPv6 ?

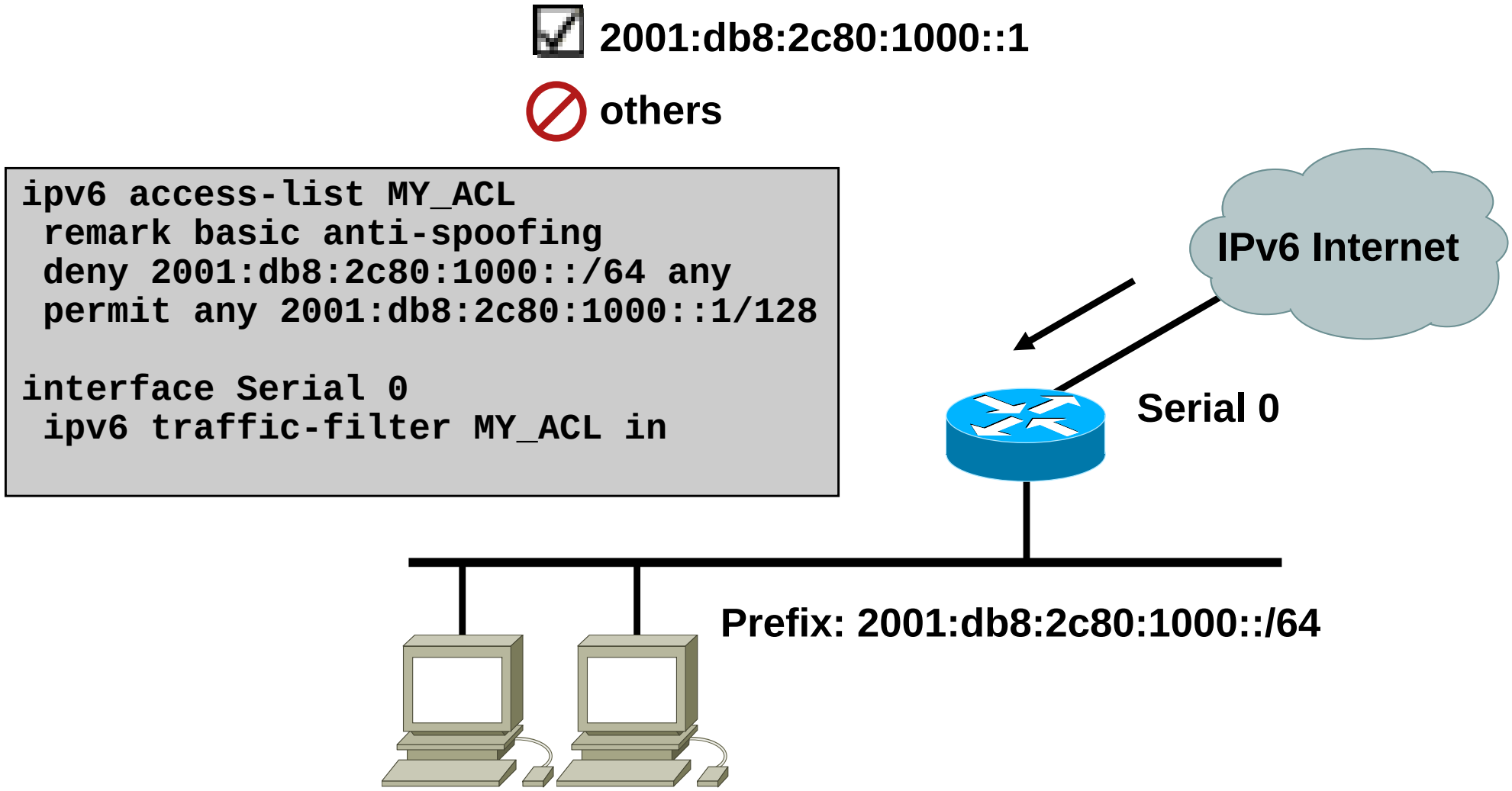
IOS IPv6 Extended ACL



- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - ICMPv6 code and type
  - Traffic class (only six bits/8) = DSCP
  - Flow label (0-0xFFFFF)
- IPv6 extension header
  - **`routing`** matches any RH, **`routing-type`** matches specific RH
  - **`mobility`** matches any MH, **`mobility-type`** matches specific MH
  - **`dest-option`** matches any, **`dest-option-type`** matches specific destination options
  - **`auth`** matches AH
  - Can skip AH (but not ESP) since IOS 12.4(20)T
- **`fragments`** keyword matches
  - Non-initial fragments (same as IPv4)
  - And the first fragment if the L4 protocol cannot be determined
- **`undetermined-transport`** keyword matches (only for deny)
  - Any packet whose L4 protocol cannot be determined: fragmented or unknown extension header

Cisco IOS IPv6 ACL
A Trivial Example

Filtering inbound traffic to one specific destination address



IPv6 ACL Implicit Rules

- Implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Be careful when adding « **deny ipv6 any any log** » at the end

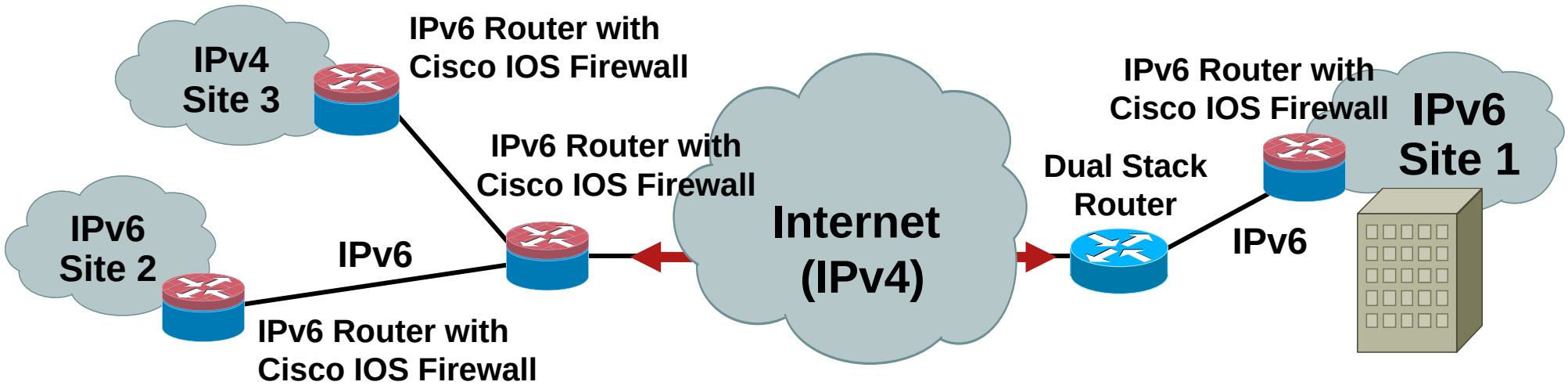
```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```

Example: RFC 4890 ICMP ACL

```
ipv6 access-list RFC4890
    permit icmp any any echo-reply
    permit icmp any any echo-request
    permit icmp any any 1 3
    permit icmp any any 1 4
    permit icmp any any packet-too-big
    permit icmp any any time-exceeded
    permit icmp any any parameter-problem
    permit icmp any any mld-query
    permit icmp any any mld-reduction
    permit icmp any any mld-report
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any router-solicitation
```

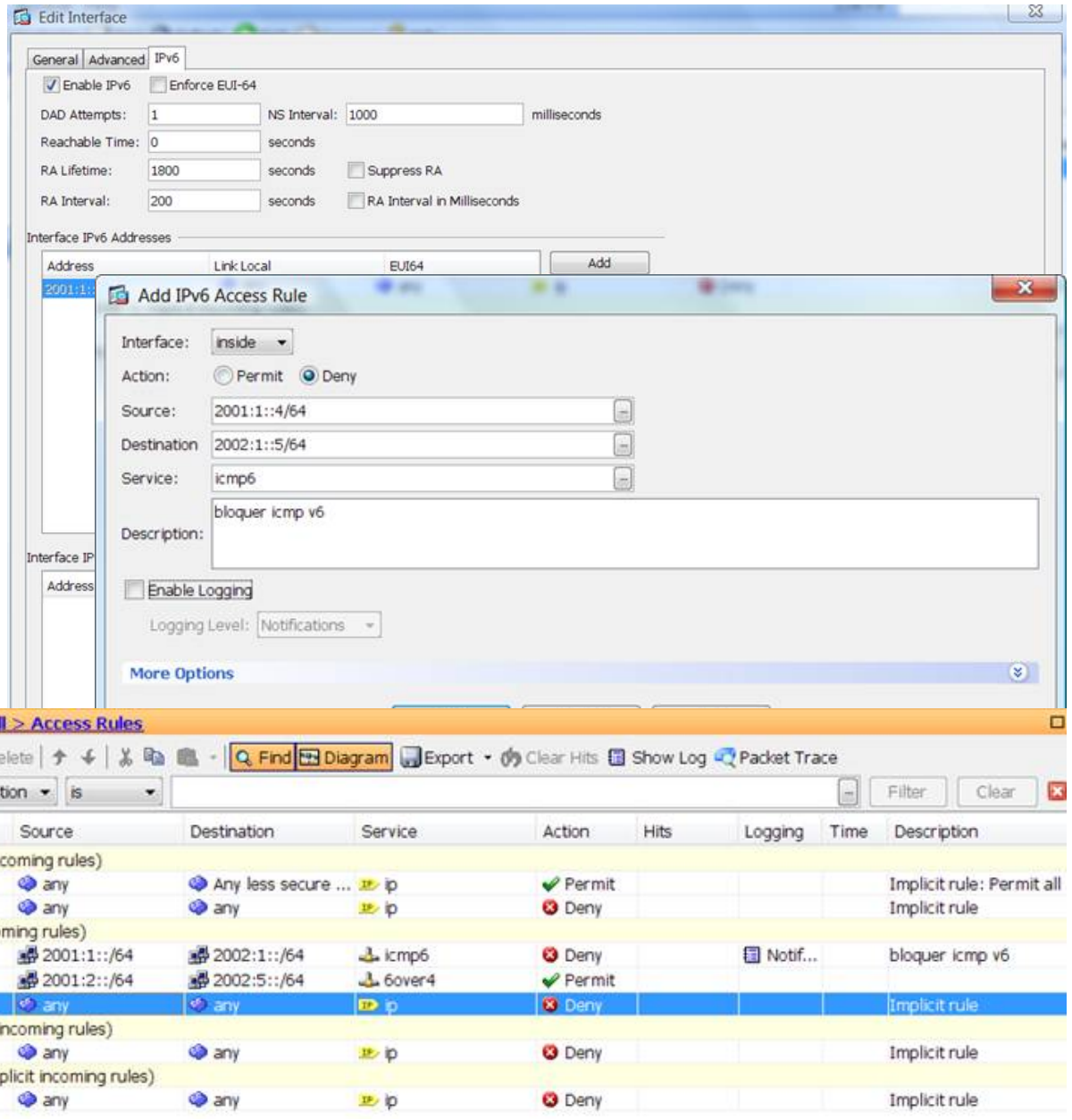
Cisco IOS Firewall IPv6 Support

- Stateful protocol inspection (anomaly detection) of IPv6 fragmented packets, TCP, UDP, ICMP and FTP traffic
- IOS 12.3(7)T (released 2005)
- Stateful inspection of IPv4/IPv6 packets
- IPv6 DoS attack mitigation
- Recognizes IPv6 extension headers



ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6 only, IPv4 only
- Extended IP ACL with stateful inspection
- Application awareness
  - HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks
- Management access
  - Telnet, SSH, HTTP
- ASDM support (ASA
- Routed & transparen (ASA 8.2)
- Caveat: no fail-over s



ASA 7.x: ACL
Very Similar to Cisco IOS

For Your Reference

```
interface Ethernet0
 nameif outside
 ipv6 address 2001:db8:c000:1051::37/64
 ipv6 enable
interface Ethernet1
 nameif inside
 ipv6 address 2001:db8:c000:1052::1/64
 ipv6 enable

ipv6 route outside ::/0 2001:db8:c000:1051::1

ipv6 access-list SECURE permit tcp any host
2001:db8:c000:1052::7 eq telnet
ipv6 access-list SECURE permit icmp6 any
2001:db8:c000:1052::/64

access-group SECURE in interface outside
```

ASA 7.x: Stateful Inspection

For Your Reference

```
ASA# show conn
4 in use, 7 most used
ICMP out fe80::206:d7ff:fe80:2340:0 in
fe80::209:43ff:fea4:dd07:0 idle 0:00:00 bytes 16
UDP out 2001:db8:c000:1051::138:53 in
2001:db8:c000:1052::7:50118 idle 0:00:02 flags -
TCP out 2001:200:0:8002:203:47ff:fea5:3085:80 in
2001:db8:c000:1052::7:11009 idle 0:00:14 bytes 8975 flags
UfFRIO
TCP out 2001:db8:c000:1051::1:11008 in
2001:db8:c000:1052::7:23 idle 0:00:04 bytes 411 flags UIOB
```

Summary of Cisco IPv6 Security Products

- ASA Firewall
  - Since version 7.0
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 (ASA 8.0)
  - No stateful-failover (coming)
- FWSM
  - IPv6 in software...
- Cisco Security Agent
  - Since version 6.0.1 for IPv6 network protection
- IPS
  - Since 6.2 (November 2008)

Secure IPv6 over IPv4/6 Public Internet

- No traffic sniffing
- No traffic injection
- No service theft

Public Network	Site 2 Site	Remote Access
IPv4	▪6in4/GRE Tunnels Protected by IPsec ▪DMVPN 12.4(20)T	▪ ISATAP Protected by RA IPsec ▪ SSL VPN Client AnyConnect
IPv6	IPsec VTI 12.4(6)T	N/A

Key Take Away

- Lack of operation experience may hinder security for a while: **training is required**
- IPv6 Security enforcement is possible

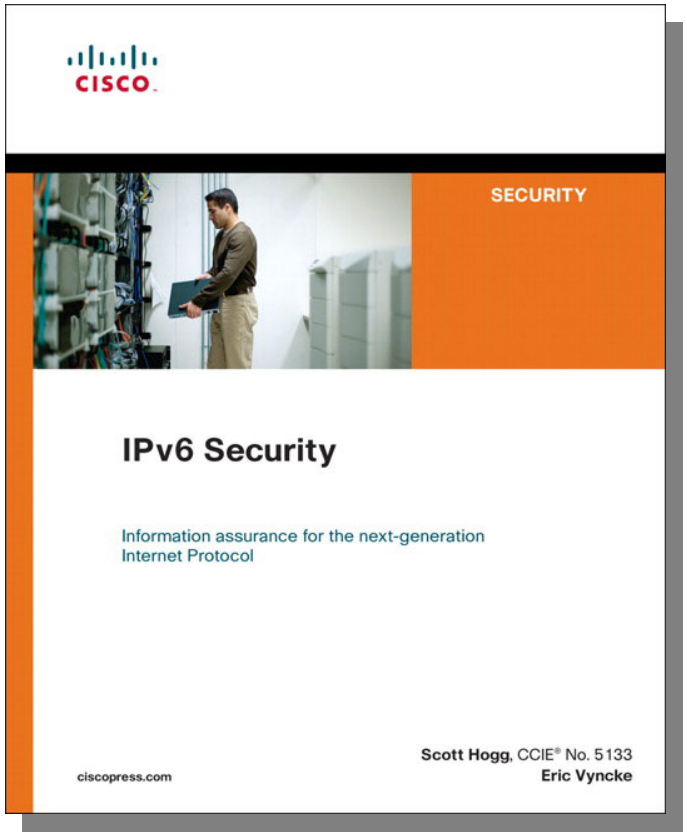
  Security policies MUST be identical for IPv4 and IPv6 (except ICMP)

  Extension Headers must be parsed

  ICMP policies are different, see RFC 4890
- Don’t wait until it is too late

Recommended Reading

Shameless plug...



Source: Cisco Press

http://www.informit.com/store/product.aspx?isbn=1587055945

Q and A

Draft IPv6 Roadmap

IPv6 Business Information Exchange

April 21, 2009

Nalini Elkins

www.insidethestack.com

(831) 659-8360

ROADMAP ENVIRONMENT

- IPv4 network services provider (NSP)
- NSP customers are networks of individual users, and application data centers
- NSP users access applications across the network
- No control over when or if customers will convert to IPv6
- Application conversion is outside the scope

ROADMAP OBJECTIVES

- Do a high-level plan, that shows the major tasks/steps
- Do a high-level timeline, that shows chronological order & relative duration

AGENDA

- Roadmap Goals – Are these the right goals?
- Roadmap Tasks – Are these the right tasks?
- Roadmap Timeline – Is this a useful way to represent a roadmap?

ROADMAP GOALS

Design Goals

- Become an IPv6 LIR
  Why: Ability to assign IPv6 /48s to our customers.

- Use an IPv6 Globally Routable Addresses (GRA)
  Why: Avoid unregistered Unicast Local Addresses (*ULAs).*

- Maintain IPv4 services & service levels
  Why: No control over when and if customers will convert.

ROADMAP GOALS

Design Goals (Cont)

- IPv6 services transparent to IPv4 customers
  Why: No control over when and if customers convert

- IPv6 services supported – IPv6 to IPv4, IPv6 to IPv6
  Why: When customers are ready to do IPv6, we will be ready too.

- Same SLAs apply to IPv6, including security
  Why: Avoid customer surprises.

ROADMAP GOALS

Implementation Goals

- Establish a target implementation date
- Factor in HW/SW/Docs upgrades
- Factor in resource constraints
- Factor in training needs
- Factor in Business Drivers

ROADMAP TASKS

Pre-Design Task

- Assess Vulnerability (DoS, Security) of IPv4 Network to IPv6 Traffic

ROADMAP TASKS

Design Tasks

- Verify Assumptions
- Define IPv6 Services
- Define IPv6 Security Requirements
- Develop a High-Level Design

ROADMAP TASKS

Design Tasks (Cont)

- Assess DNS / DHCPv6 changes for Support of IPv6
- Implement Test Lab
- Test Design in the Lab
- Finalize the Design

ROADMAP TASKS

Implementation Tasks

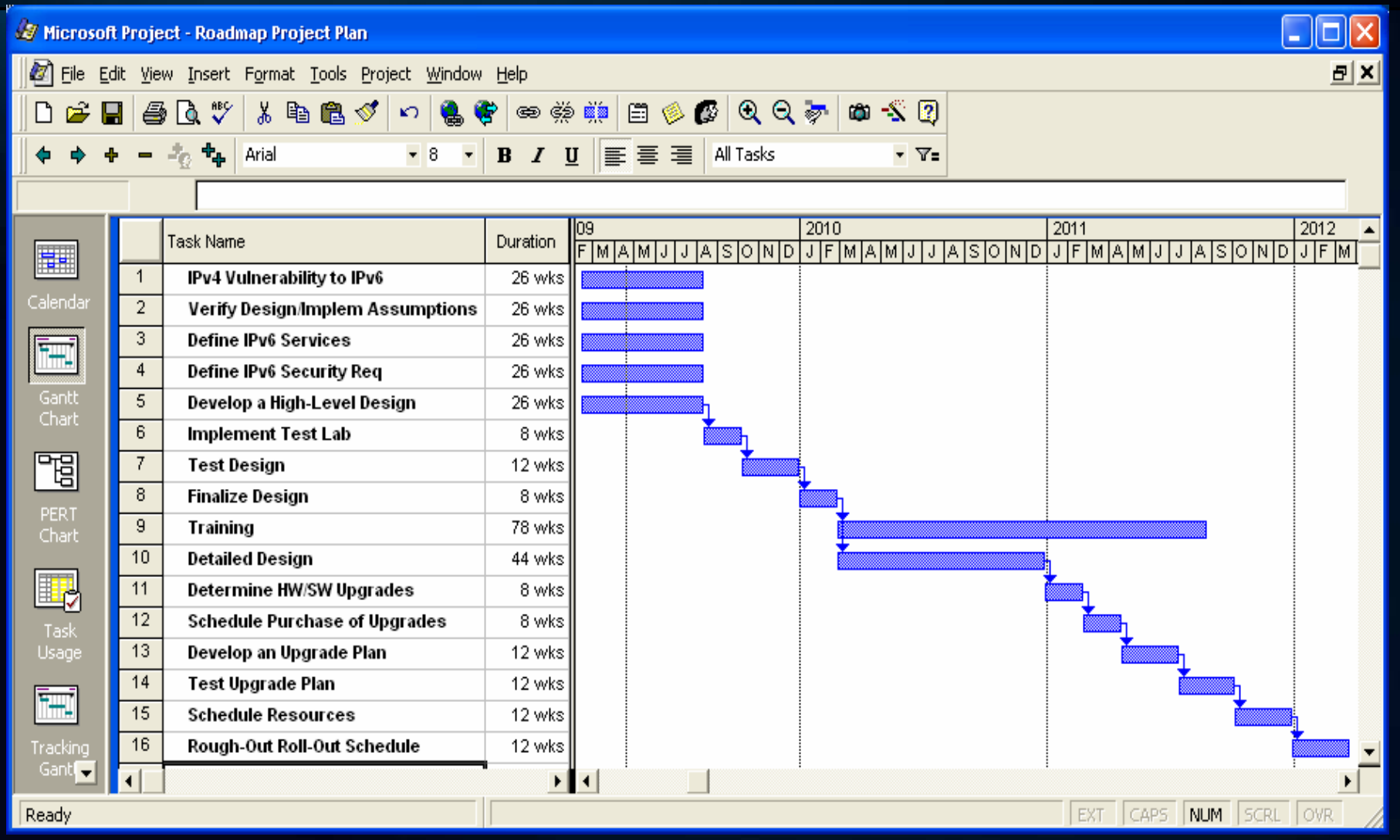
- Plan/Execute IPv6 Training
- Develop Detailed Design Specs
- Determine HW/SW Upgrades (consider budget process)
- Schedule Purchase of Upgrades

ROADMAP TASKS

Implementation Tasks (Cont)

- Develop Upgrade Plan
- Test Upgrade Plan
- Schedule Resources
- Rough-Out Rollout Schedule

ROADMAP TIMELINE



KEY QUESTION

- Is this a useful approach for a Roadmap?