FORTINET®

Security Implications of Migrating to IPv6

Patrick Bedwell

VP, Product Marketing

December 14, 2011

Agenda

1. Why It’s Important
2. Network Security Vendors & IPv6 Readiness
3. IPv6 Threats
4. Planning the Migration
5. Q & A

Reasons Why You Should Care

- IPv6 is “New”
  - What happened the last time you let something new in your network?

- IPv6-Compatible Systems are in Your Network Today
  - You may be the last one to find out

- It May be New to Your Security Vendor Too
  - Support varies widely between vendors
  - Performance & functionality implications

IPv6 Security Concerns

- 2010 Survey of 111 Network Operators
- Greatest Concerns:
  - Misconfiguration
  - Lack of visibility
  - Lack of v4/v6 feature parity

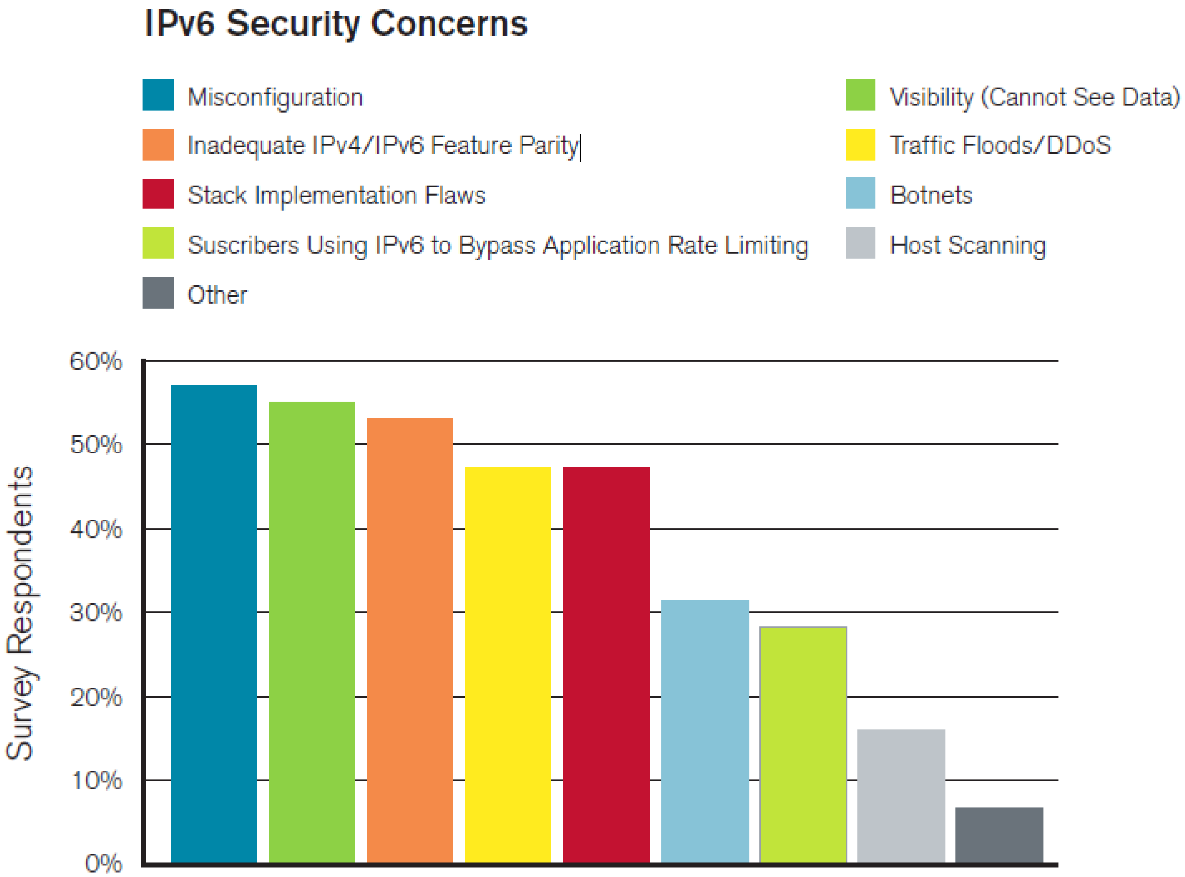


Figure 58

Source: Arbor Networks, Inc.

IPv6 Adoption To-Date

- No Consensus
  - Other than “It’s increasing”
- Tipping Point?
  - Content providers
  - Network providers
  - Federal governments

- Network World Survey of 210 IT Departments – July ‘11
  - 72% will upgrade web sites by 2013
  - 65% will upgrade internal network by 2013
  - 46% found ‘most’ HW & SW supports IPv6

IPv6 Certifications

Cert	Fortinet	Competitors						
		A	B	C Series 1	C Series 2	D	E	F
JITC	🟢	🔴	🔴	🟢	🔴	🔴	🔴	🔴
USGv6	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🔴
IPv6 Ready Phase 2	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢

- **Joint Infrastructure Task Force**
  - Part of DoD Unified Capabilities Requirements
- **National Institute of Standards & Technology**
  - Standards & testing to support adoption of IPv6 in US Gov't
- **IPv6 Ready Logo Program**
  - Verify protocol implementation and validate interoperability

The State of the Security Industry

- Wide Range of IPv6 Support
  - Many vendors do not support or only partially supported
  - Limited model support for several vendors
  - Some vendors require purchase of additional modules
  - Primarily software implementation, not HW accelerated

Feature	Fortinet	Competitors				
		A Series 1	A Series 2	D	F Series 1	F Series 2
Firewall	🟢	🔴	🟢	🔴	🔴	🟢
Content Security	🟢	🔴	🔴	🔴	🔴	🔴
Virtual Appliances	🟢	🔴	🟢	🔴	🔴	🔴

Some Common IPv6 Security Myths

- IPv6 Will Reduce the Number of Attacks
  - Threats are not going away because of new protocol
  - Malware via IPv4 = Malware via IPv6
- IPsec Encrypts All Traffic
  - Potential for Authentication, Data protection, etc.
  - Reality: Not being used due to complexity
- Not Deploying IPv6 Will Prevent Access to IPv6 Content
  - Work-arounds are easy for motivated users
    - E.g., 6to4 translation in a Mac or Teredo for Windows

Common Threats

- Tunneling of IPv6 across IPv4
  - IPv6 traffic ignored
    - Bypass content filtering / flow controls
      - E.g. Teredo function within Windows 7/ Vista
  - Likely threats
    - C & C traffic for botnets
    - File sharing
    - Deliver malware to IPv4 network
  - Solution
    - Unified Threat Management / Next Generation Firewall with native IPv6 support

- Type O Routing Header
  - Specify routers along path to use
  - Likely threat
    - Target routers for DOS attack
  - Solution
    - DoS protection in the Firewall
    - Drop packets traversing a forwarding device that contain the Type 0 Routing Header

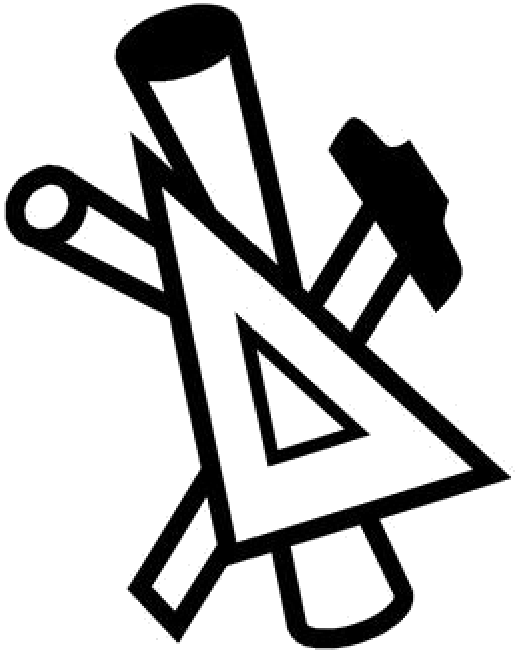
Common Threats (continued)

- Deployment of 6-to-4 gateways and carrier-grade NATs
  - Workaround for not deploying native IPv6 support
  - Threat
    - DDoS
    - Obfuscation
  - Solution
    - Strong gateway security

- Rogue Devices
  - Stateless Router Auto-config feature of IPv6
  - Threat
    - Enables rogue device to assign IPv6 addresses in your network
  - Solution
    - Strong Gateway Security
    - Use of DHCPv6

A Security Perspective on Your Migration Planning

- The Plan
  1. Develop a plan for your IPv6 transition mechanism
  2. Train your staff
  3. Review the plan again
  4. Inventory infrastructure, ID incompatible hardware, replace
  5. Test, test and test again
  6. Do a pilot
  7. Install, configure, debug new infrastructure



- Security Perspective
  1. Get moving
  2. Start with your incompatible firewall & replace it right away
  3. Ensure parity with existing IPv4 infrastructure
  4. Conduct regular vulnerability assessments

Goal: IPv6 Visibility & Control

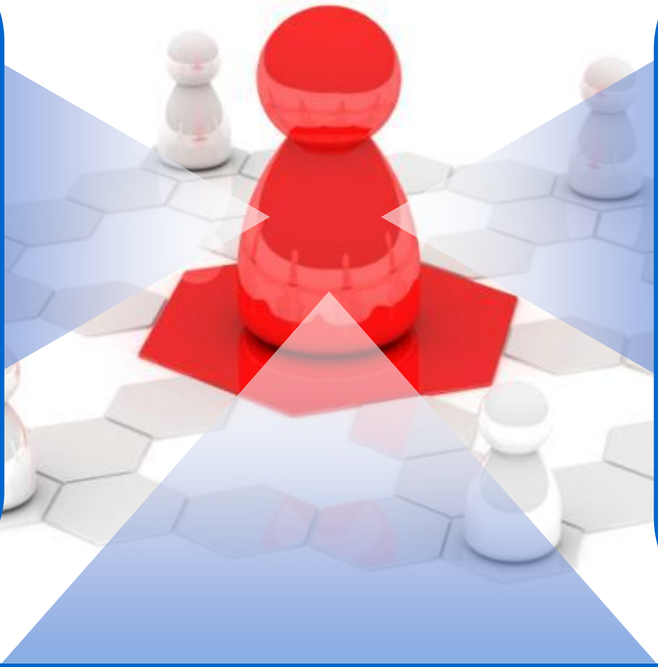
- Content
  - Understand what's in your network
  - Block unwanted / malicious content
  - Prioritize delivery
  - Limit access by groups or users
    - Time of day, day of week

- Apps & Features within Apps
  - Categories of apps
  - Individual apps
  - Actions within apps
- Users
  - Domain, groups, individuals
  - Mobile devices

Goal: IPv6 Multi-Threat Protection

Connection Security

- **Firewall**
  "External" threat protection
- **Endpoint**
  App control +
  VPN for secure private traffic across public networks



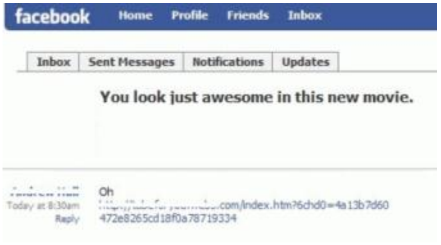
Application Security

- **Web filtering**
  Protection from harmful web sites and web content
- **Application Control**
  Restrict access to unacceptable applications

Content Security

- **Intrusion Prevention (IPS)**
  Monitoring and active protection from malicious traffic
- **Antivirus/ Antimalware**
  Detection and removal of malicious application content

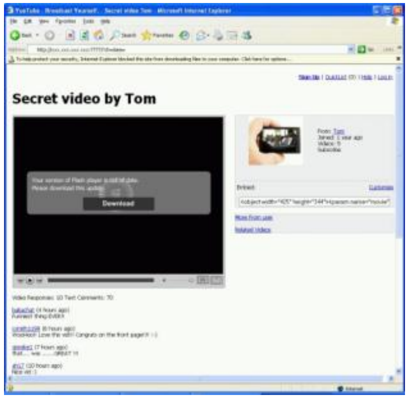
Result: Integrated IPv6 Content Security



You look just awesome in this new movie.

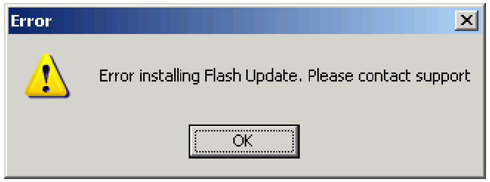
Oh
Today at 8:30am
Reply
.com/index.htm?6chd0=4a13b7d60
472e8265cd18f0a78719334

"Innocent" Video Link:
Redirects to malicious Website


Secret video by Tom

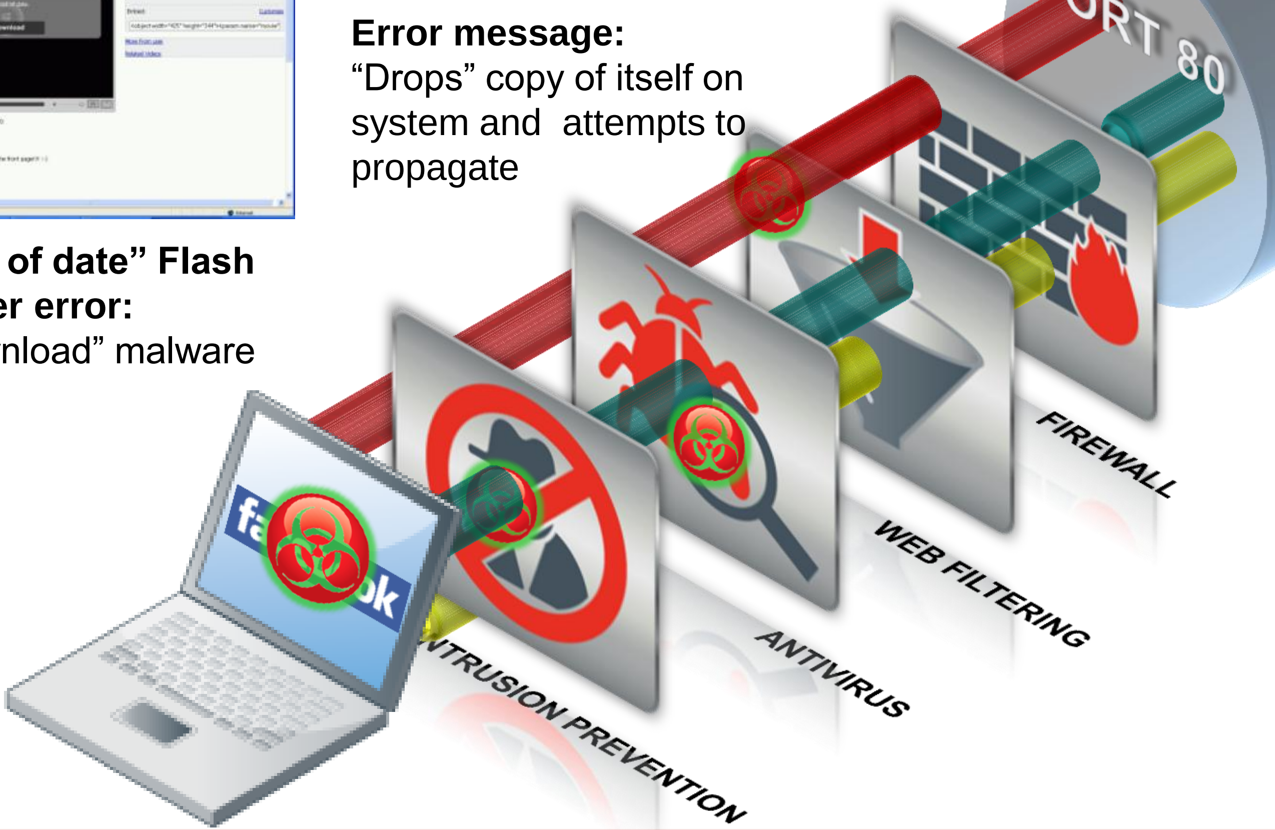
Your version of Flash player is out of date.
Please download this update

"Out of date" Flash player error:
"Download" malware file



Error installing Flash Update. Please contact support

Error message:
"Drops" copy of itself on system and attempts to propagate



Integrated Web Filtering
Blocks access to malicious Website

Network Antivirus
Blocks download of virus

Intrusion Protection
Blocks the spread of the worm

FORTINET®

Thank You

Patrick Bedwell
pbedwell@fortinet.com