Check Point
SOFTWARE TECHNOLOGIES LTD.

SWISS IPv6 COUNCIL

IPv6 SECURITY

CHALLENGES & SOLUTIONS

AVIV **ABRAMOVICH**

Check Point
SOFTWARE TECHNOLOGIES LTD.

IPv6 Security Challenges

Main IPv6 security challenges

Check Point
SOFTWARE TECHNOLOGIES LTD.

IPv6 as a Covert Channel for Malware

Vulnerabilities in IPv6 Mechanisms

Transition and Tunneling Mechanisms

IPv6 as Covert Channel for Malware

Check Point SOFTWARE TECHNOLOGIES LTD.

IPv6 Enabled by Default

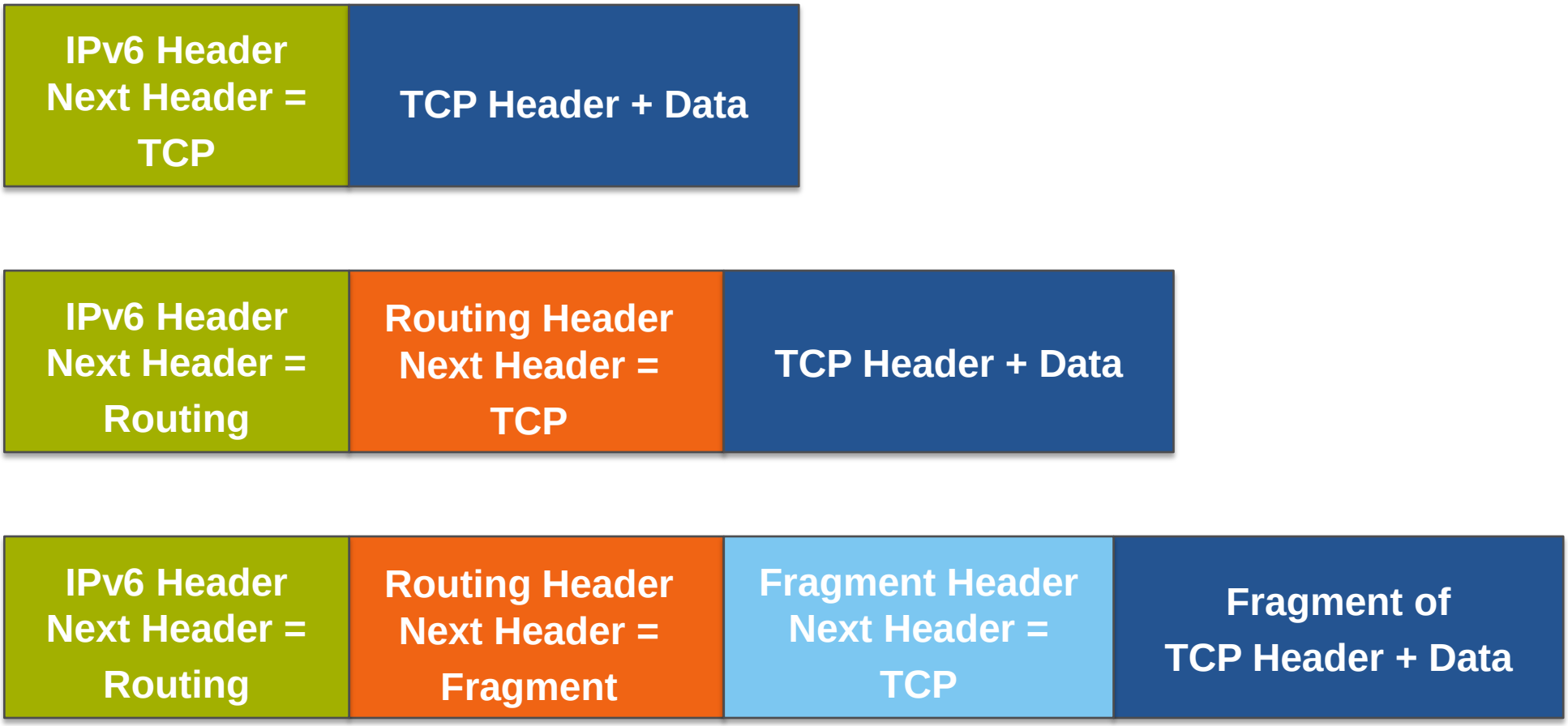
- Most host Operating systems enable IPv6 by default
- It's easy to create IPv6 / IPv4 tunnels to carry traffic outside of an enterprise
- Windows Vista/7 can do this automatically

IPv6 Running Now

- Set up by users who want to try IPv6
- Could be used as covert channel by botnets and malware

You can't stop what you can't see

Vulnerabilities in IPv6 Mechanisms



Examples

- CVE-2014-2309

The ip6_route_add function in net/ipv6/route.c in the **Linux kernel** through 3.13.6 does not properly count the addition of routes, which allows remote attackers to cause a denial of service (memory consumption) via a flood of ICMPv6 Router Advertisement packets.

- CVE-2014-0254 (MS14-006)

The IPv6 implementation in **Microsoft Windows 8**, **Windows Server 2012**, and **Windows RT** does not properly validate packets, which allows remote attackers to cause a denial of service (system hang) via crafted ICMPv6 Router Advertisement packets, aka "TCP/IP Version 6 (IPv6) Denial of Service Vulnerability.“

Security must provide specific defense against attacks on these vulnerabilities

Transition & Tunneling Mechanisms

Check Point SOFTWARE TECHNOLOGIES LTD.

IPv6 in IPv4 Tunnel RFC4213

IPv4 in IPv6 Tunnel RFC2473

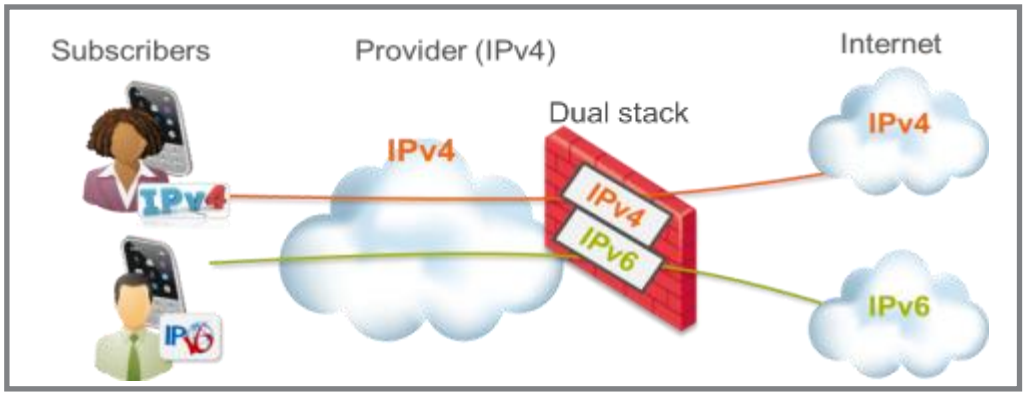
Tunneling IPv6 over UDP through NAT RFC4380

IPv6 Security Solutions

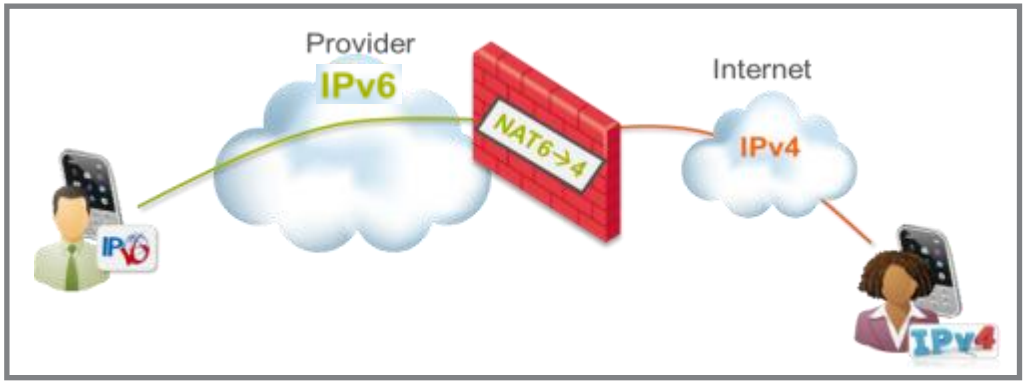
IPv6 Deployment Scenarios

IPV4 to IPv4 connection

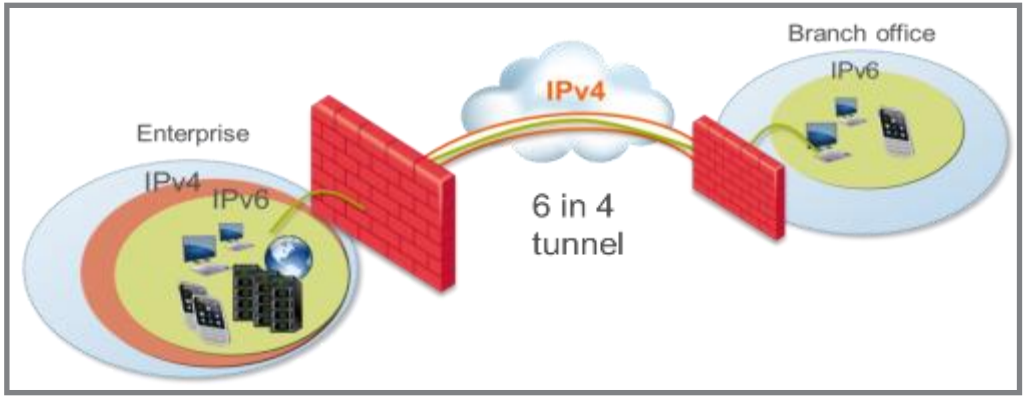
IPv6 to IPv6 connection



IPV6 to IPv4 connection



IPV6 to IPv6 connection
(over IPv4)



IPv6 Deployment Recommendations

Check Point
SOFTWARE TECHNOLOGIES LTD.

Create IPv6 Security Policy that Parallels IPv4 Security Policy

Protect Against Rogue Router Advertisements and DHCPv6 Servers

Set Up Default Firewall Rules that Block Undesired Tunnels

IPv6 Security Policy

Parallel IPv4 Policy	▪ All objects should have IPv6 information ▪ Basic rules should be implemented for IPv4 and IPv6 ▪ Specific rules for IPv6 where necessary
Verify	▪ Rules are implemented in extensions headers ▪ Rules are implemented in tunneled traffic

Rogue Router Advertisements and DHCPv6 Servers

Check Point SOFTWARE TECHNOLOGIES LTD.

Rogue RA & DHCPv6

- Easy to turn host into Router via Connection Sharing
- Unauthorized Access Points & Routers (plugged in backwards)
- Similar problems with DHCPv4

Solutions

- Identify host and port using IPS
- Disable port at L2 switch (or physically)

Default Rules to Block Undesired Tunnels

Check Point SOFTWARE TECHNOLOGIES LTD.

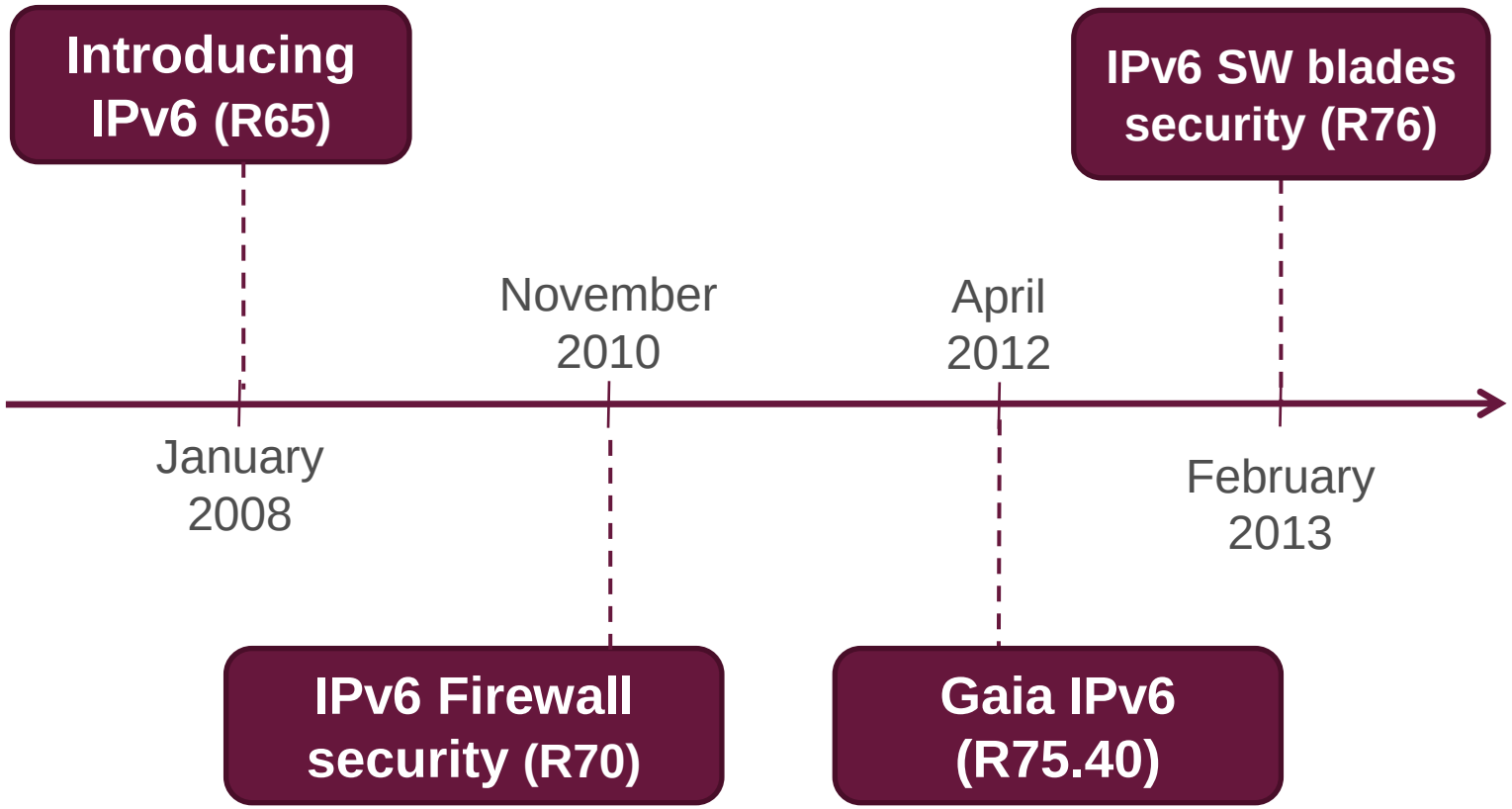
Block Tunnels by Default

- Turn off host based tunnels by default
- Only authorized tunnels should be allowed
- Configured and Automatic tunnels

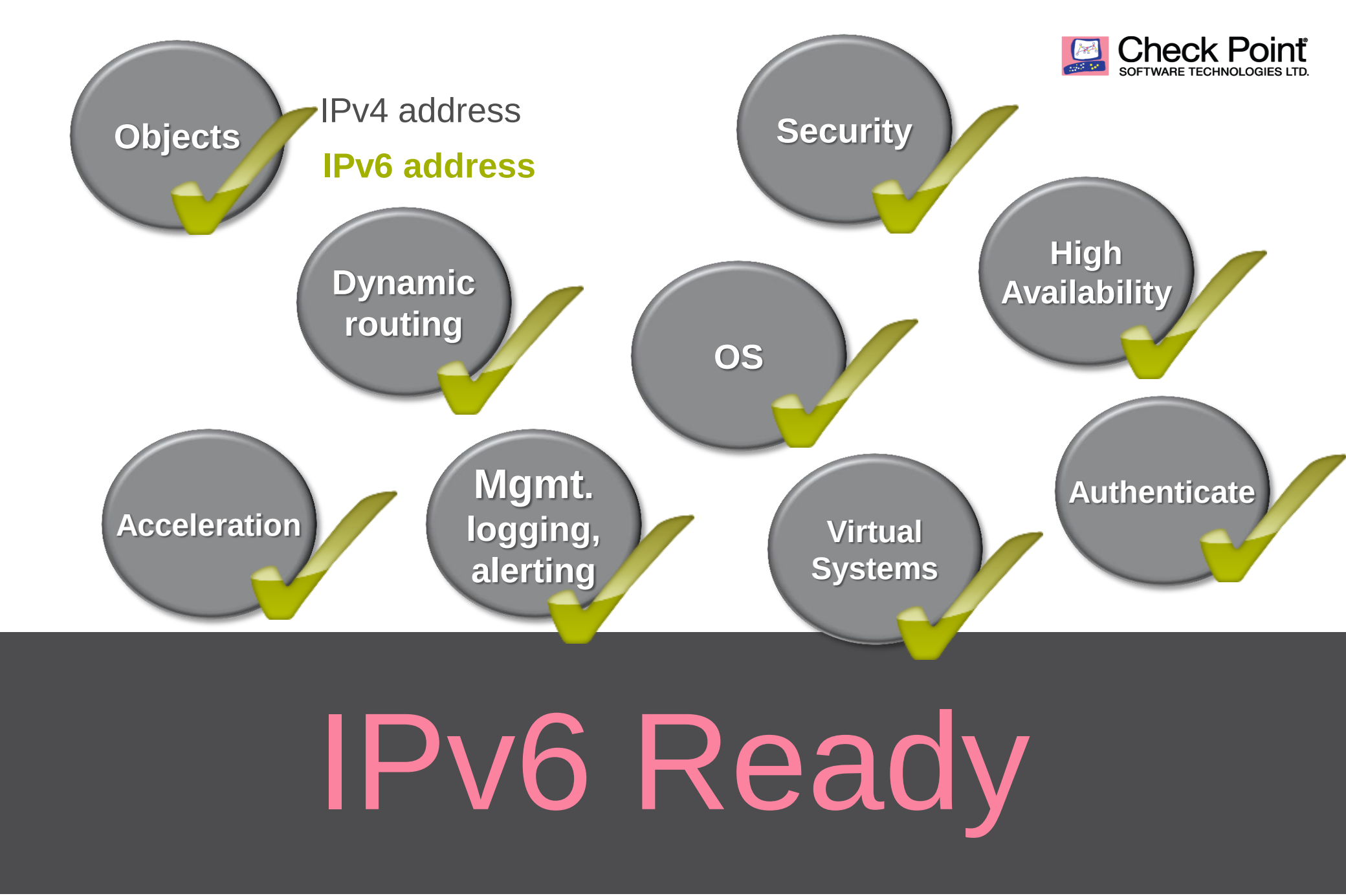
Examples

- Block IPv6 in IPv4 from any SRC to any DST
- Allow IPv6 in IPv4 from <Router A> to <Tunnel Broker B>
- Block IPv4 in IPv6 from any SRC to any DST
- Block IPv6 over IPv4 from any SRC to any DST
- ……

Check Point IPv6 Commitment



Continuous IPv6 evolution adapted to the industry needs



What's Next

Still some gaps (www.ripe.net/ripe/docs/ripe-554)

- ✓ IPv6 Basic specification [RFC2460] (FW, IPS, APFW)
- ✓ IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- ✗ Default Address Selection [RFC3484] (FW, IPS, APFW)
- ✓ ICMPv6 [RFC4443] (FW, IPS, APFW)
- ✓ SLAAC [RFC4862] (FW, IPS)
- ✓ Deprecation of Type 0 Routing Headers in IPv6 [RFC5095]
- ✓ Inspecting IPv6-in-IPv4 protocol-41 traffic, which is specified in: Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (IPS)
- ✓ Router-Alert option [RFC2711] (FW, IPS)
- ✓ Path MTU Discovery [RFC1981] (FW, IPS, APFW)
- ✓ Neighbor Discovery [RFC4861] (FW, IPS, APFW)
- ✓ If the request is for the BGP4 protocol, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545 (FW, IPS, APFW)
- ✓ If the request is for a dynamic internal gateway protocol (IGP), then the required RIPng [RFC2080], OSPF-v3 [**RFC5340**] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
- ✗ If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- ✗ Support for QoS [RFC2474, RFC3140] (FW, APFW)
- ✓ If tunneling is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW)

Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU