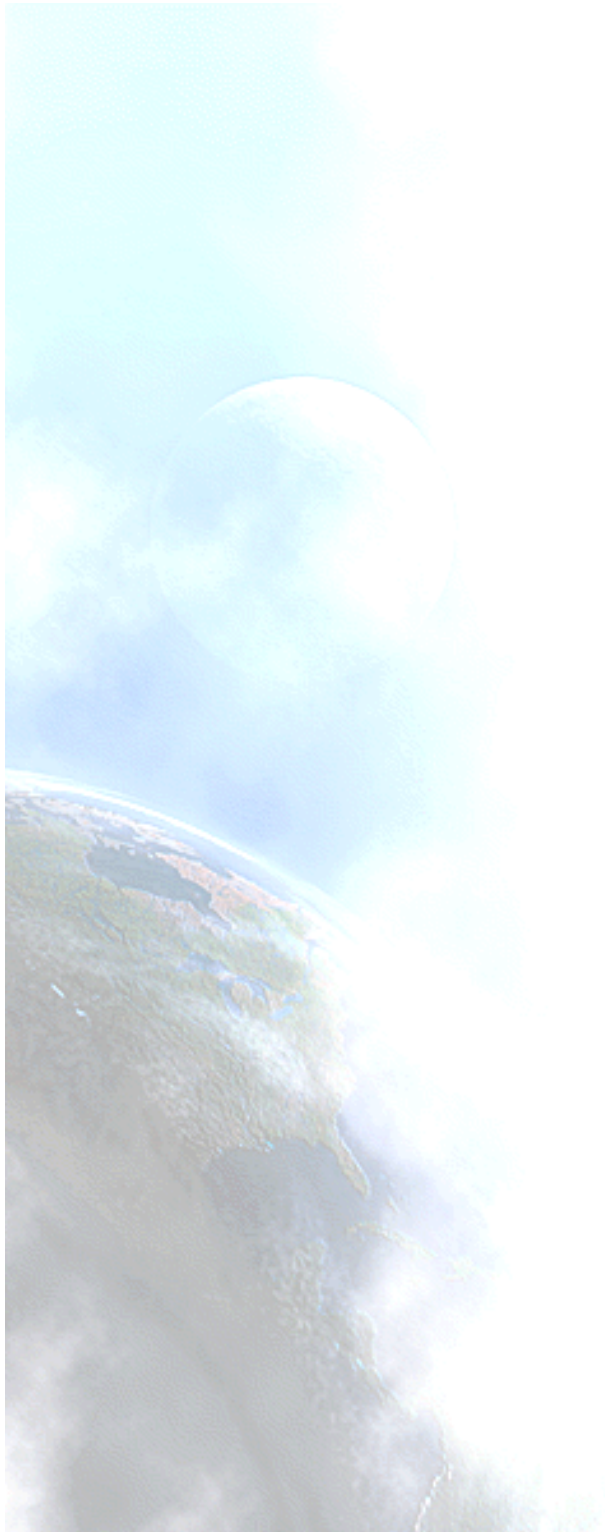
IPv6 Security

APNIC 44
Taichung - Taiwan
September 2017

Jordi Palet (jordi.palet@theipv6company.com)

Introduction

- Although Security is a vast field, here only IPv6-related issues will be introduced.
- First IPsec will be described because of its mandatory implementation on all IPv6 stacks. This will provide security services to all IPv6 devices.
- Then some concrete security solutions that have been developed within IPv6 context will be treated: Privacy extensions and SEND.
- IPv6 will be compared with IPv4 from the threats point of view.
- At the end a general analysis will be given from a practical point of view, comparing IPv4 and IPv6 security issues.
- Last but not least, the Distributed Security Model will be introduced.



IPsec

IP Security (IPsec)

- **Goals**:
  - Provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6.
  - Not adversely affect users, hosts, and other Internet components that do not employ IPsec for traffic protection.
  - Security protocols (AH, ESP and IKE) are designed to be cryptographic algorithm independent. A set of default algorithms are defined.
- **Security Services Set**:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Protection against replays (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality.

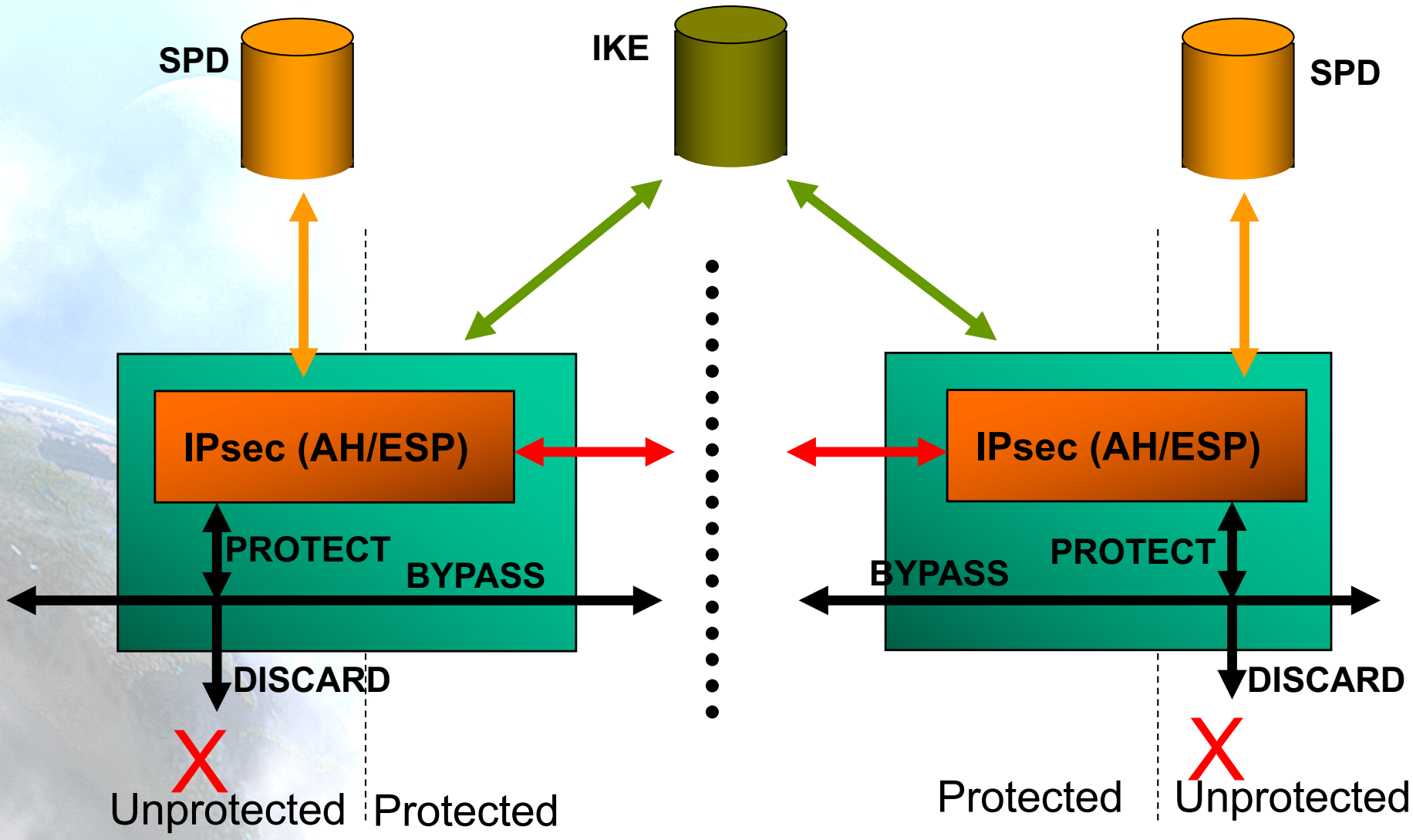
IPsec: Basic elements

- Basic elements:
  - **Base architecture** for IPsec compliant systems [RFC4301].
  - **Security Protocols:** Authentication Header (AH) [RFC4302] and Encapsulating Security Payload (ESP) [RFC4303].
  - **Security Associations:** What they are and how they work, how they are managed, associated processing [RFC4301].
  - **Key Management**: Manual and automatic (The Internet Key Exchange IKE) [RFC4306].
  - **Algorithms for authentication and encryption**: Mandatory, default, algorithms are defined for use with AH and ESP [RFC4835] and for IKEv2 [RFC4307].

System Overview (1)

- An IPsec implementation operates in a host, as a security gateway (SG) or as an independent device.
- The protection offered by IPsec is based on requirements defined by a Security Policy Database (SPD).
- Packets are matched based on IP and next layer header information against entries in the SPD.
- Each packet is either PROTECTed using IPsec security services, DISCARDed, or allowed to BYPASS IPsec protection.
- IPsec can be used to protect one or more "paths“ (a) between a pair of hosts, (b) between a pair of security gateways, or (c) between a security gateway and a host.

System Overview (2)



Security Protocols

- IPsec implementations MUST support ESP and MAY support AH. AH and ESP may be applied alone or in combination with each other
- **AH** provides:
  - Integrity.
  - Data origin authentication.
  - Optional (at the discretion of the receiver) anti-replay features.
- **ESP** provides:
  - Integrity.
  - Data origin authentication.
  - Optional (at the discretion of the receiver) anti-replay features.
  - Confidentiality (NOT recommended without integrity).
- Both offers access control, enforced through the distribution of cryptographic keys and the management of traffic flows as dictated by the Security Policy Database.
- These mechanisms are designed to be algorithm-independent.

SA: The Concept

- Security Association (SA) is a fundamental concept for IPsec:
  - **A simplex "connection" that affords security services to the traffic carried by it.**
- AH & ESP use SA's, so all implementations MUST support the concept of a Security Association.
- A major function of IKE is the establishment and maintenance of Security Associations.
- To secure typical, bi-directional communication between two IPsec-enabled systems, a pair of SAs (one in each direction) is required. IKE explicitly creates SA pairs.

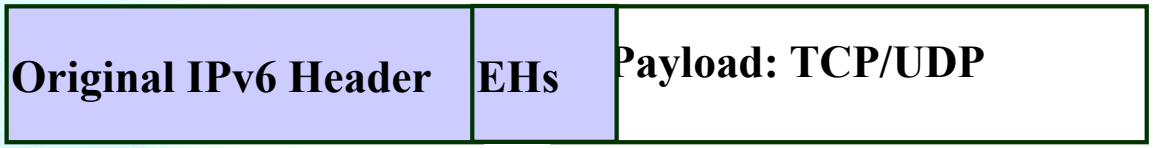
SA Identification

- Each SA is uniquely identified by a triple:
  - Security Parameter Index (SPI)
    - Bit String Assigned to the SA (local meaning), as a pointer to a SA Database (SPD or Security Policy Database).
  - IP Destination Address
  - Security protocol (AH or ESP) identifier
- Destination Address may be:
  - Unicast Address
  - IP broadcast address
  - Multicast group address

Modes of Use

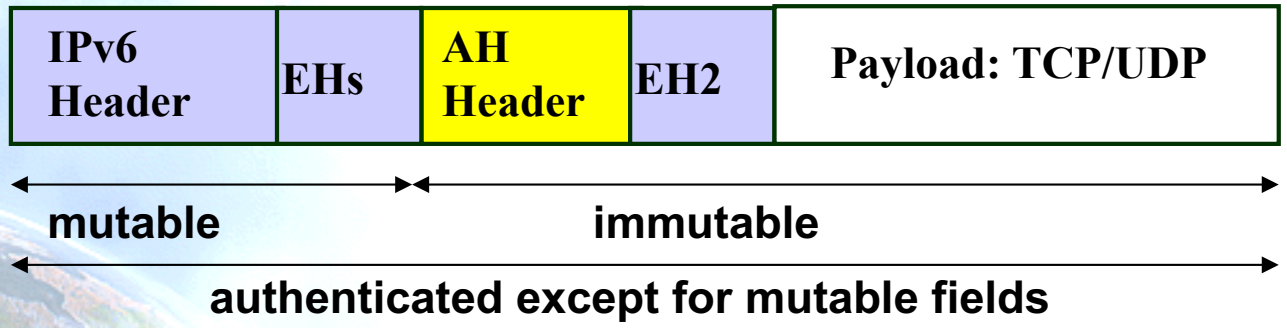
- Each protocol supports two modes of use:
  - Transport mode (protection primarily for upper layer protocols)
    - Direct between end-to-end systems
    - Both Remote systems must support IPsec !
  - Tunnel mode (protocols applied to tunneled IP packets)
    - Secure tunnel for encapsulating insecure IP packets
    - Between intermediate systems (not end-to-end)

AH in Transport and Tunnel Mode

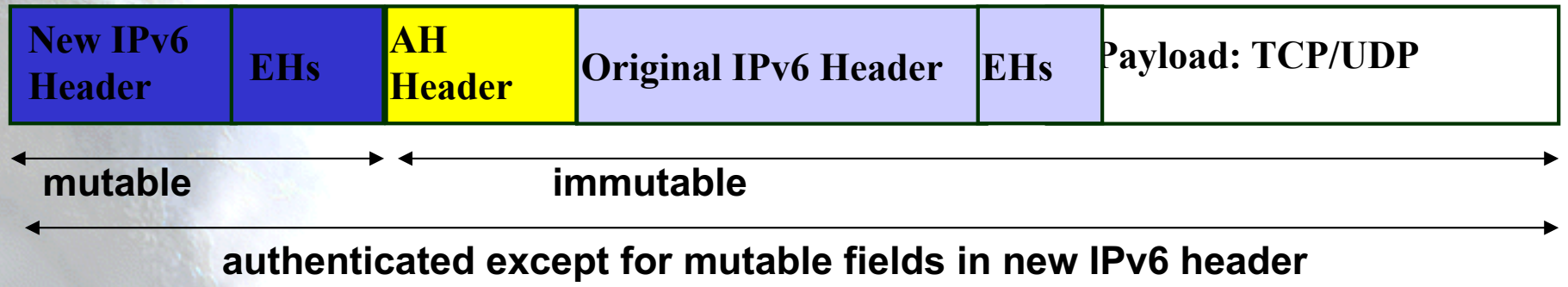


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

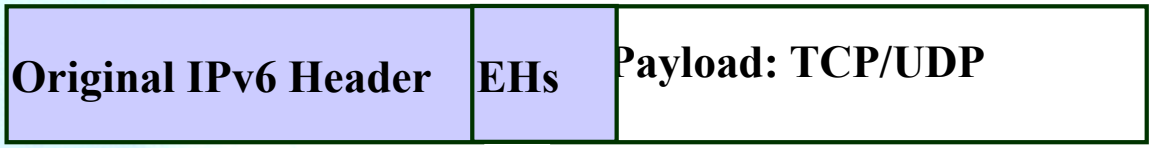
Transport Mode



Tunnel Mode

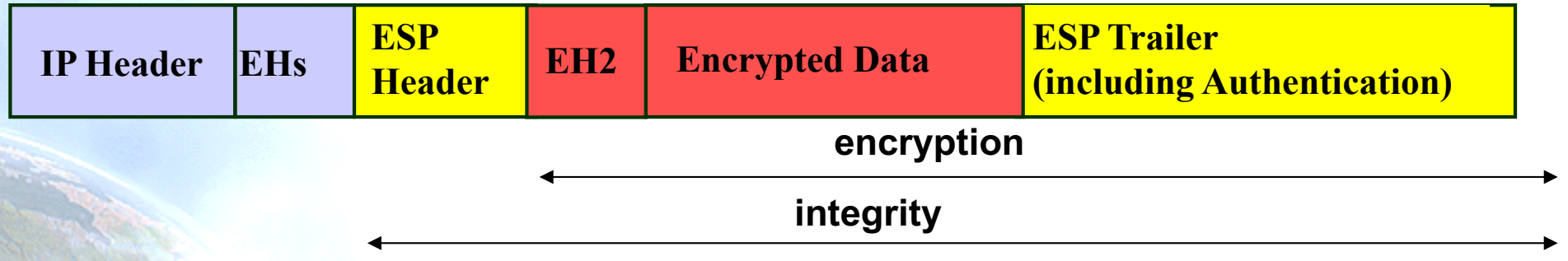


ESP in Transport and Tunnel Mode

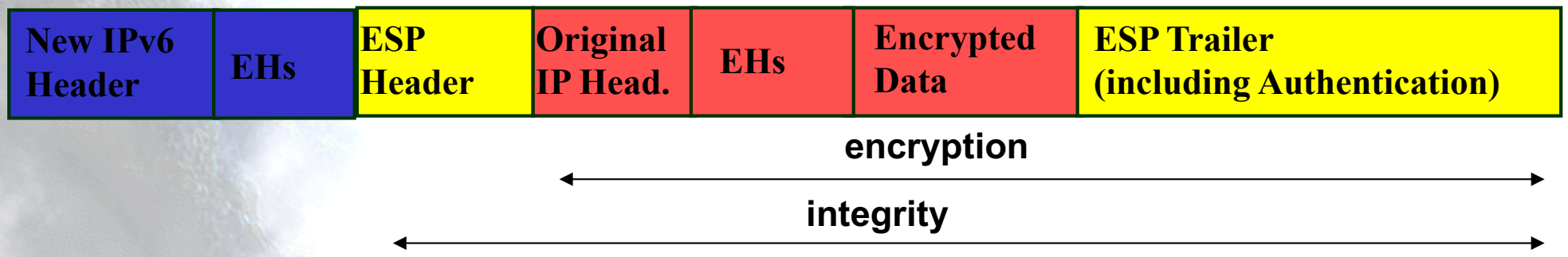


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

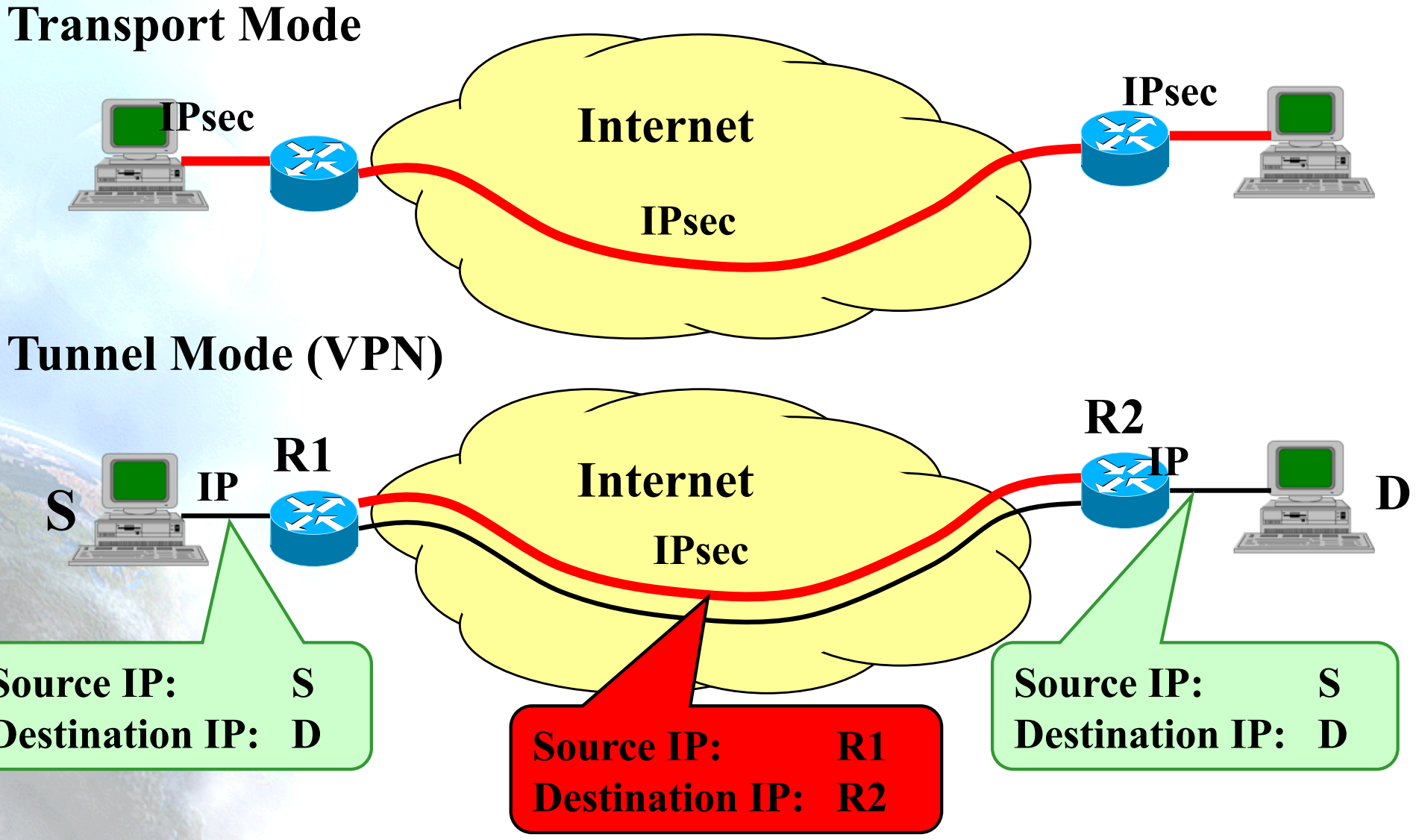
Transport Mode



Tunnel Mode



Transport vs. Tunnel Mode



Privacy Extensions

Why Privacy Extensions ?

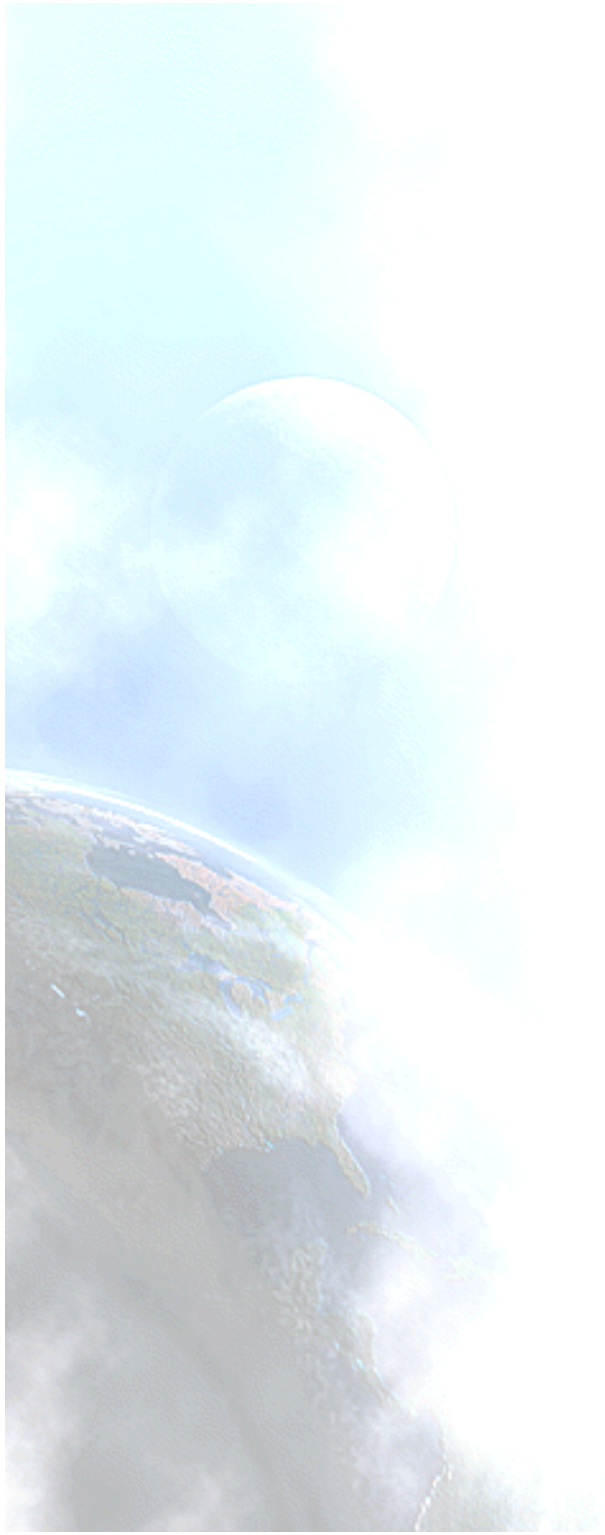
- Issue
  - The IPv6 addresses on a given interface generated via Stateless Autoconfiguration contain the same interface ID, regardless of where within the Internet the device connects. This facilitates the tracking of individual devices
- Possible Solutions
  - Use DHCP for obtaining addresses. The DHCP server could arrange to hand out addresses that change over time
  - Change the interface ID portion of an address over time and generate new addresses from the interface ID for some address scopes

Privacy Extensions (1)

- RFC4941 describes an extension to IPv6 stateless address autoconfiguration that makes nodes to generate global-scope addresses that change over time.
- RFC4941 is based on generate random interface identifiers with limited life-time.

Privacy Extensions (2)

- Almost all OSs, use a random IID, that changes over time
  - In some cases this is undesirable, because ti makes more difficult network administration (log inspection, firewalling, etc.)
- Some OSs (like Windows 7) use an alternative method:
  - IID is generated using a hash function over the network prefix
  - For a given prefix, IPv6 addresses don't change
  - If prefix changes, IID changes
  - This option have "the best of both worlds"



ND Threats

Overview

- The Neighbor Discovery (ND) [RFC4861] Protocol is vulnerable to various attacks [RFC3756].
- Original ND Protocol specification defines the use of IPsec to protect ND messages. Form many reasons in practice this is not a solution.
- SEcure Neighbor Discovery (SEND) [RFC3971], explained before, aims to protect ND Protocol.

ND Threats (1)

- Neighbor Solicitation/Advertisement Spoofing.
  - Done by either sending a Neighbor Solicitation with a different source link-layer address option, or sending a Neighbor Advertisement with a different target link-layer address option.
  - This is a redirect/DoS attack.
- Neighbor Unreachability Detection (NUD) failure.
  - A malicious node may keep sending fabricated NAs in response to NUD NS messages. Unless the NA messages are somehow protected, the attacker may be able to extend the attack for a long time using this technique.
  - This is a DoS attack.

ND Threats (2)

- Duplicate Address Detection DoS Attack.
  - An attacking node could launch a DoS attack by responding to every duplicate address detection attempt made by an entering host.
  - The attacker can claim the address in two ways: it can either reply with an NS, simulating that it is performing DAD, too, or it can reply with an NA, simulating that it has already taken the address into use.
  - May also be present when other types of address configuration is used, i.e., whenever DAD is invoked prior to actually configuring the suggested address.
  - This is a DoS attack.

ND Threats (3)

- Malicious Last Hop Router.
  - An attacking node on the same subnet as a host attempting to discover a legitimate last hop router could masquerade as an IPv6 last hop router by multicasting legitimate-looking IPv6 Router Advertisements or unicasting Router Advertisements in response to multicast Router Advertisement Solicitations from the entering host.
  - The attacker could ensure that the entering host selected itself as the default router by multicasting periodic Router Advertisements for the real last hop router having a lifetime of zero. This may spoof the entering host into believing that the real access router is not willing to take any traffic.
  - This threat is a redirect/DoS attack.

ND Threats (4)

- Default router is 'killed‘.
  - An attacker 'kills' the default router(s), thereby making the nodes on the link to assume that all nodes are local.
  - The attacker can launch a classic DoS attack against the router so that it does not appear responsive any more. The other is to send a spoofed Router Advertisement with a zero Router Lifetime.
- Good Router Goes Bad.
  - A router that previously was trusted is compromised.
  - The case of “Malicious Last Hop Router” applies.
  - This is a redirect/DoS attack.

ND Threats (5)

- Spoofed Redirect Message.
  - The attacker uses the link-local address of the current first-hop router in order to send a Redirect message to a legitimate host.
  - Since the host identifies the message by the link-local address as coming from its first hop router, it accepts the Redirect.
  - As long as the attacker responds to Neighbor Unreachability Detection probes to the link-layer address, the Redirect will remain in effect.
  - This is a redirect/DoS attack.

ND Threats (6)

- Bogus On-Link Prefix.
  - An attacking node can send a Router Advertisement message specifying that some prefix of arbitrary length is on-link.
  - If a sending host thinks the prefix is on-link, it will never send a packet for that prefix to the router. Instead, the host will try to perform address resolution by sending Neighbor Solicitations, but the Neighbor Solicitations will not result in a response, denying service to the attacked host.
  - This attack can be extended into a redirect attack if the attacker replies to the Neighbor Solicitations with spoofed Neighbor Advertisements.
  - This is a DoS attack.

ND Threats (7)

- Bogus Address Configuration Prefix.
  - An attacking node can send a Router Advertisement message specifying an invalid subnet prefix to be used by a host for address autoconfiguration.
  - As a result, return packets never reach the host because the host's source address is invalid.
  - This attack has the potential to propagate beyond the immediate attacked host if the attacked host performs a dynamic update to the DNS based on the bogus constructed address.
  - This is a DoS attack.

ND Threats (8)

- Parameter Spoofing.
  - An attacking node could send out a valid-seeming Router Advertisement that duplicates the Router Advertisement from the legitimate default router, except the included parameters are designed to disrupt legitimate traffic.
  - Specific attacks include:

1. Include a Current Hop Limit of one or another small number which the attacker knows will cause legitimate packets to be dropped before they reach their destination.
2. The attacker implements a bogus DHCPv6 server or relay and the 'M' and/or 'O' flag is set, indicating that stateful address configuration and/or stateful configuration of other parameters should be done. The attacker is then in a position to answer the stateful configuration queries of a legitimate host with its own bogus replies.

  - This is a DoS attack.

ND Threats (9)

- Replay attacks.
  - All Neighbor Discovery and Router Discovery messages are prone to replay attacks.
  - An attacker would be able to capture valid messages and replay them later.
  - In request-reply exchanges, such as Solicitation-Advertisement, the request may contain a nonce that must appear also in the reply. Old replies are not valid since they do not contain the right nonce.
  - Stand-alone messages, such as unsolicited Advertisements or Redirect messages, may be protected with timestamps or counters.

ND Threats (10)

- Neighbor Discovery DoS Attack.
  - The attacking node begins fabricating addresses with the subnet prefix and continuously sending packets to them. The last hop router is obligated to resolve these addresses by sending NS packets.
  - A legitimate host attempting to enter the network may not be able to obtain ND service from the last hop router as it will be already busy with sending other solicitations.
  - This DoS attack is different from the others in that the attacker may be off-link.

RA Problems

- If there are multiple nodes sending Ras with prefixes for SLAAC, could result in a DoS attack

(RFC6104, Rogue IPv6 Router Advertisement Problem Statement, Feb. 2011)

- Different solutions:
  - RA-GUARD (RFC6105, IPv6 Router Advertisement Guard, Feb. 2011)
  - RAMOND: http://ramond.sourceforge.net -> Send RA with zero lifetime, or change priority of legitimate RA to high
  - SEND

RA-GUARD

- Several organizations use RA-Guard as a first line of defense against rogue RAs
- This is a filtering policy applied on switches
- RA-Guard works (mainly) this way:
  - The switch is configured to accept Ras only on specified port(s)
  - RAs received in other ports are discarded
  - RA-Guard assumes that the switch could identify the RA messages

IPv4 vs. IPv6 Threat Analysis

Overview

- **Security:** include several procedures, mechanisms, best common practices and tools.
- With **IPv6** there will be several points that will be the same as with IPv4, i.e., they are “IP-independent”. E.g. firmware and software updates or application level security risks.
- IPv6 introduces new considerations to be taken into account. We will see that they could derive in advantages or drawbacks.

IPv6 Security: first contact

- The first two ideas that come to a security responsible when deploying IPv6 are:
  1. Global addresses are used (there is the exception of ULAs), i.e., they are globally reachable from everywhere in the Internet, in other words, **there is no NAT**.
  2. All IPv6 stacks must support IPsec, as seen previously.
- The first could give a false feeling of “danger” and the second a false impression of protection. These will be explained later.

Security Threats Classification

- Three categories of IPv6 threats could be established:
  1. Threats that already existed with IPv4 and have similar behavior with IPv6.
  2. Threats that already existed with IPv4 and have new considerations with IPv6.
  3. New threats that appear with IPv6.

IPv4 threats with similar behavior with IPv6

- **Sniffing:** IPsec could help.
- **Application Layer Attacks**: IPsec can be used to trace the attacker, although introduces a problem for IDS. Application layer protection could be used too.
- **Unauthorized Devices**: They pretend to be switches, routers, access points, or resources such as DNS, DHCP, or AAA servers.
- **Man-in-the-Middle Attacks**: IPsec could help.
- **Flooding Attacks**.

IPv4 threats with different behavior with IPv6 (1)

- **Network Scanning**: The typical network (/64) scanning is in practice much less feasible. Also automated attacks, e.g. network worms that pick random host addresses to propagate to, may be hampered.
- **Broadcast-Amplification Attacks (Smurf)**: DoS attack. An ICMP echo is sent to the broadcast address of a prefix with the spoofed address of the victim. All hosts on the destination prefix in turn send an echo reply to the victim. **In IPv6, there is no concept of broadcast.**

IPv4 threats with different behavior with IPv6 (2)

- **Transition-Mechanism Attacks**: No new technologies used, same type of vulnerabilities than with IPv4. Issues:
  - Dual-stack networks could be attacked over both protocols
  - IPv6 tunneling need new ports to be open on firewalls

  Recommendations:
  - On dual-stack network/hosts implement similar security measures for both IPv4 and IPv6.
  - Control the use of tunnels whenever possible.
  - Enable firewalls to inspect encapsulated traffic.

New IPv6 Threats

- ND Threats
- Routing Header Type 0 [RFC5095]
- Transition mechanisms, in the sense that they work encapsulating traffic and the firewalls and other security software must be able to process it
- IPsec, in the sense of sending encrypted data that firewalls can't inspect, especially full-state firewalls

IPv6 security issues

IPv6 security issues (1)

- **IPsec**: As said above IPsec is (NO MORE) mandatory on all IPv6 implementations. This could give a false “security feeling”, because IPsec provides security only if it is used. In practice IPsec is not widely deployed and used because the lack if an Internet-wide key exchange mechanism.

  IPsec is configured manually in some concrete and controlled configurations, this is not scalable.

  Another point to be taken into account is that IPsec traffic could not be inspected by firewalls.

IPv6 security issues (2)

- **End-to-end**: The use of global IPv6 addresses **allows but do not force** every node to be reachable. The network/security administrator could decide if all, some or none traffic could reach each part of the network.

  Different scenarios:

  - **DSL subscriber**: The traffic should reach the CPE with no interference. The user has the responsibility to filter in the CPE.
  - **Data Center**: Controlled environment where only allowed services should be deployed.

IPv6 security issues (3)

- The **new addressing scheme** implies that:
  - The **number of addresses** is REALLY big. Brute force/random scanning makes no sense [RFC5157].
  - Each node could have **several addresses** and even random interface identifiers [RFC4941]. This makes difficult to control a host by its IP.
  - The use of link-local addresses on an IPv6 interface allows for IP connectivity on a LAN segment without any external help. As a guide you should not trust on sessions coming from link-local addresses and allow them only for basic services.
  - Well known multicast addresses are defined so that services could be located. This also eases the work to find sensible services to attack (FF05::2 All routers, FF05::1:3 All DHCP Servers).

IPv6 security issues (4)

- **Extension headers (EH)**: this powerful and flexible mechanism should be taken into account by security devices, i.e. they should be able to inspect the EH chain.
- **Fragmentation**: In IPv6 only the end hosts could fragment a packet. This reduce possible attacks using fragment overlap or tiny fragments. Consideration for out of order fragments are the same as in IPv4 but on the end node. Firewalls should not filter packet fragments.

IPv6 security issues (5)

- **Autoconfiguration:** In IPv6 different methods for autoconfiguration are defined. DHCP has the same consideration in IPv4 and IPv6. Neighbor Discovery Protocol has several threats (as ARP in IPv4), and IPsec and SEND could be used to add security.
- **IPv6 Mobility**: IPv6 eases the Mobile IP deployment although some elements needed for a real world deployment are being defined, including security concerns.

IPv6 security issues (6)

- **Routing Header:** Type 0 Routing Header (RH0) can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating denial-of-service traffic.

  A packet can be constructed such that it will oscillate between two RH0-processing hosts or routers many times. This allows a stream of packets from an attacker to be amplified along the path between two remote routers, which could be used to cause congestion along arbitrary remote paths and hence act as a denial-of-service mechanism.

IPv6 security issues (7)

- The severity of this threat is considered to be sufficient to warrant deprecation of RH0 entirely [RFC5095].
- Only Routing Header type 0 is affected, so especifications for routing header type 2 are still valid, used in MIPv6

Practical issues

Practical Issues (1)

- **ICMPv6 is a fundamental part of IPv6**. With IPv4 a deny_all_ICMP filtering could be applied but with IPv6 this would mean the basic functionalities not to work. **RFC4890**

Type - Code	Description	Action
Type 1	Destination unreachable	ALLOW, incoming to detect some errors
Type 2	Packet too big	ALLOW, needed for PMTU discovery
Type 3 ĞCode 0	Time Exceeded	ALLOW
Type 4 ĞCode 1 y 2	Parameter problem	ALLOW, to detect some errors
Type 128	Echo reply	ALLOW to **network debug** or **Teredo**. Incoming could be allowed limiting the rate. Outgoing allow for some **known services**.
Type 129	Echo request	ALLOW to **network debug** or **Teredo**. Outgoing could be allowed limiting the rate. Incoming allow for some **known services**.
Type 130,131,132,143	Multicast listener	ALLOW if Multicast is deployed and MLD should have to traverse a Firewall
Type 133	Router Solicitation	ALLOW if the Firewall interferes on ND
Type 134	Router Advertisement	ALLOW if the Firewall interferes on ND
Type 135	Neighbor Solicitation	ALLOW if the Firewall interferes on ND
Type 136	Neighbor Advertisement	ALLOW if the Firewall interferes on ND
Type 137	Redirect	NO ALLOW
Type 138	Renumbering	NO ALLOW
Type 139	Node information Query	NO ALLOW
Type 140	Node information Reply	NO ALLOW

Practical Issues (2)

- Depending on how much control and traceability different address configuration methods should be used. From more to less:
  - Static addresses.
  - Stateful autoconfiguration: DHCPv6.
  - Stateless autoconfiguration: Interface ID from MAC Address.
  - Stateless autoconfiguration: Interface ID using privacy extensions.
- You can't filter "blindly" extension headers (in IPv4 you could do this with IP options)

Practical Issues (3)

- It is recommended to:
  - **filter non-assigned prefixes**: Easier deny all + allow legitimate. Filtering could be coarse (Allow 2000::/3 Global Unicast) or fine (2600:0000::/12, 2400:0000::/12, etc.)
  - Also ULA traffic could not traverse Internet
  - Filter at the edge of the site site-scoped multicast
  - If Multicast is deployed these prefixes should also be allowed

Action	Src	Dst	Src port	Dst port
deny	2001:db8::/32	host/net		
permit	2001::/16	host/net	any	service
permit	2002::/16	host/net	any	service
permit	2003::/16	host/net	any	service
deny	3ffe::/16	host/net	any	service
deny	any	any		

Practical Issues (4)

- Filtering of **fragmented packets**:
  - Filter fragments destined to network devices (infrastructure DoS)
  - Check fragment filtering capabilities are OK
  - Filter all fragments of less than 1280 bytes, except the last one
  - All fragments should be delivered within 60 second, if not then discard them all

Practical Issues (5)

- **Use addresses not easy to guess**, for example not use ::1 for routers or servers, to difficult the attacker's work.

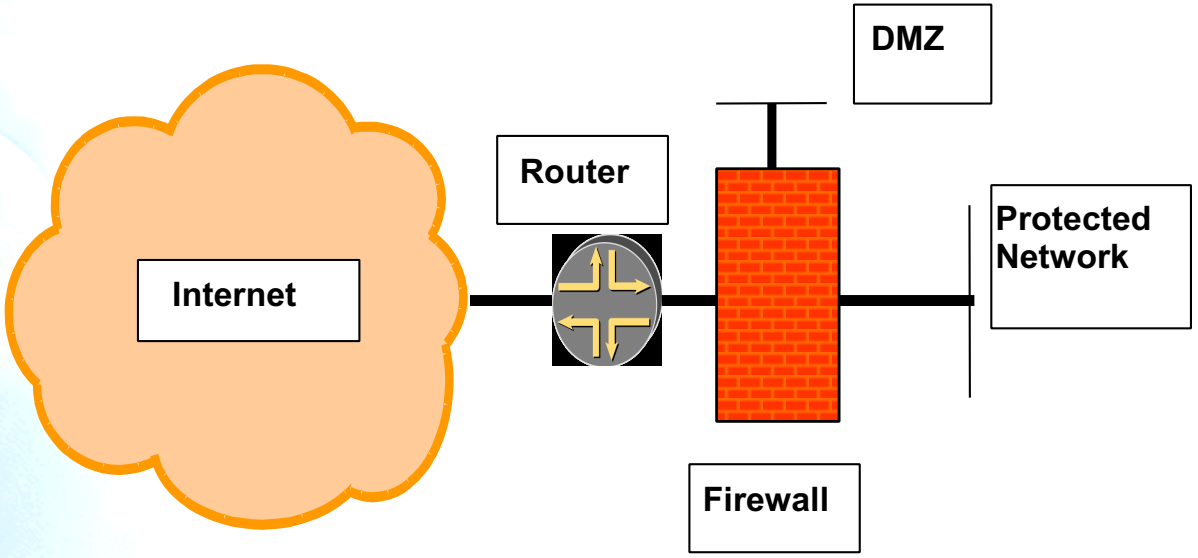
  A recommended approach is to enable stateless autoconfiguration and then use the autoconfigured address in an static assigment. This address would also be used for DNS domain name.

- **Deploy Ingress Filtering** [RFC2827, RFC3074] in a similar way as is done with IPv4.

Practical Issues (6)

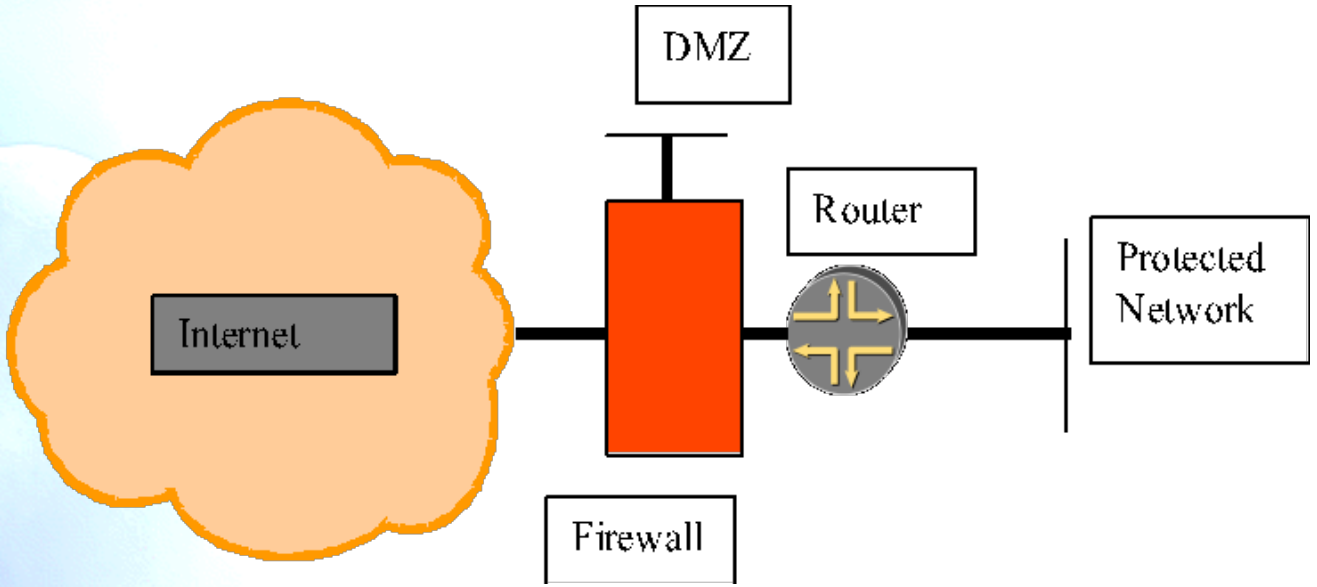
- If **transition Mechanisms** are used, be sure that the corresponding prefix is announced and its traffic is not filtered
- If you've native IPv6, secure your infrastructure against transition mechanisms.
- IPv4 and IPv6 will coexist, so the most probable scenario will be that IPv6 networks follow IPv4 networks, sharing security devices whenever it is possible. Coherent rules (do not allow everything with IPv6/nothing with IPv4)
- Make sure your firewall supports:
  - Filtering by source and destination address
  - IPv6 Extension Header processing (including RH0).
  - Filtering by upper layer protocol information
  - Encapsulated traffic inspection

Firewalls (1)



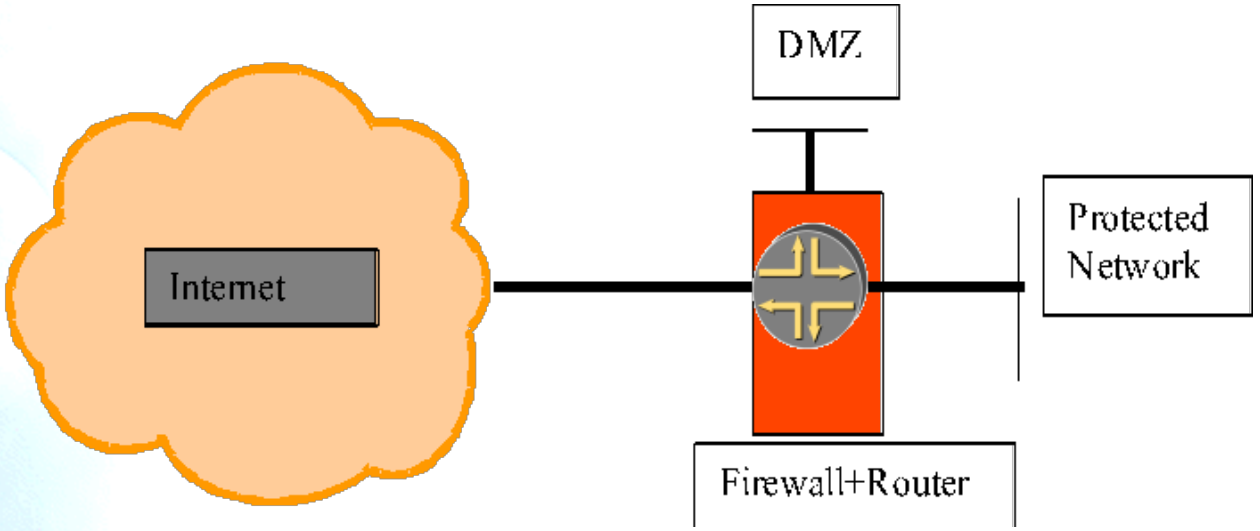
- Internet ↔ router ↔ firewall ↔ network(s)
- Requirements:
  - Firewall should support/recognize ND/NA filtering
  - Firewall should support RS/RA if SLAAC is used
  - Firewall should support MLD messages if Multicast is needed

Firewalls (2)

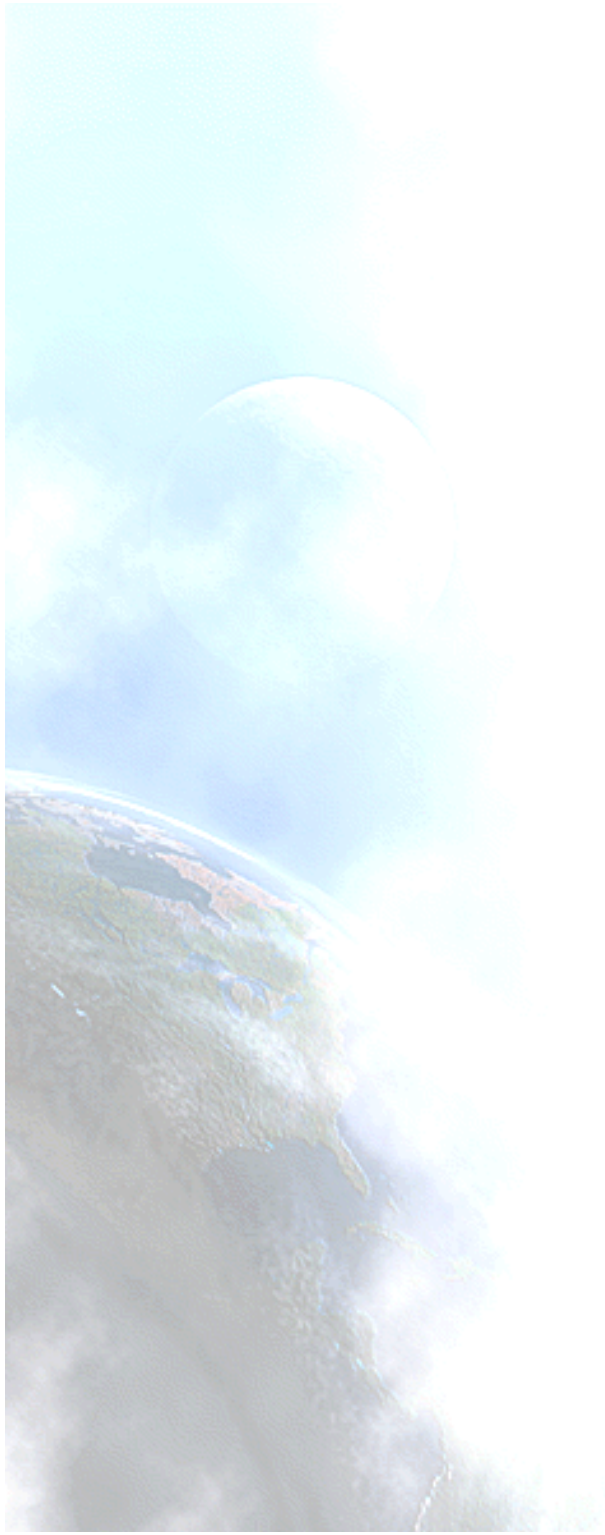


- Internet ↔ firewall ↔ router ↔ network(s)
- Requirements:
  - Firewall should support ND/NA
  - Firewall should support dynamic routing protocol filtering
  - Firewall should have great variety of interfaces

Firewalls (3)



- Internet ↔ firewall/router(edge device) ↔ network(s)
- Requirements:
  - Could be powerful – unique point for routing and security policies – very common in SOHO routers (DSL/cable)
  - Should support common routers and firewall features



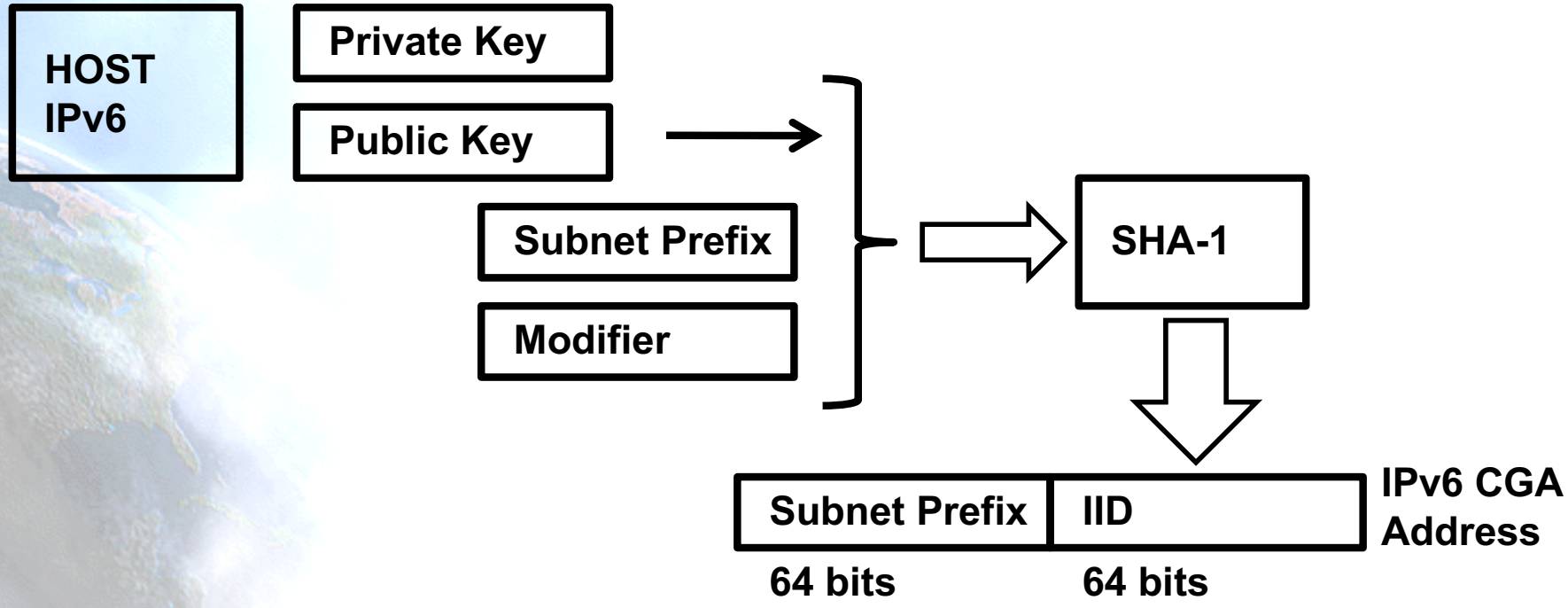
SEND

Secure Neighbor Discovery (SEND) - RFC3971

- IPv6 nodes use the Neighbor Discovery Protocol (NDP) to:
  - Discover other nodes on the link
  - Determine their link-layer addresses to find routers
  - Maintain reachability information about the paths to active neighbors
- NDP is vulnerable to various attacks if it is not secured
- RFC3971 specifies security mechanisms for NDP
  - Unlike those in the original NDP specifications, these mechanisms do not use IPsec
  - SEND is applicable in environments where physical security on the link is not assured (such as over wireless) and attacks on NDP are a concern
- Implementations are available only for linux ans *BSD:
  - E.g., http://www.docomolabs-usa.com/lab_opensource.html

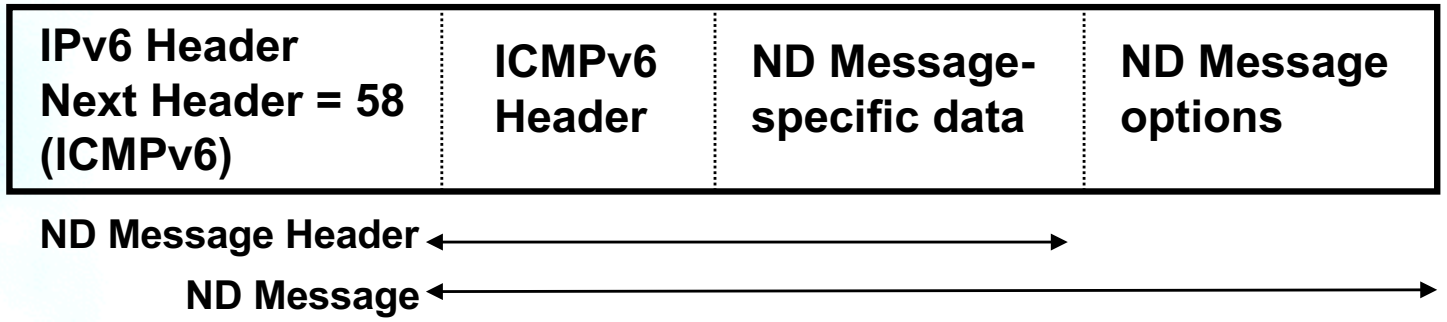
SEND and CGAs

- A host that implements SEND use a **public-private** key pair
- SEND is based in the use of CGAs [RFC3972]: IPv6 address with IID cryptographically generated using public key, network prefix and a modifier



SEND Elements

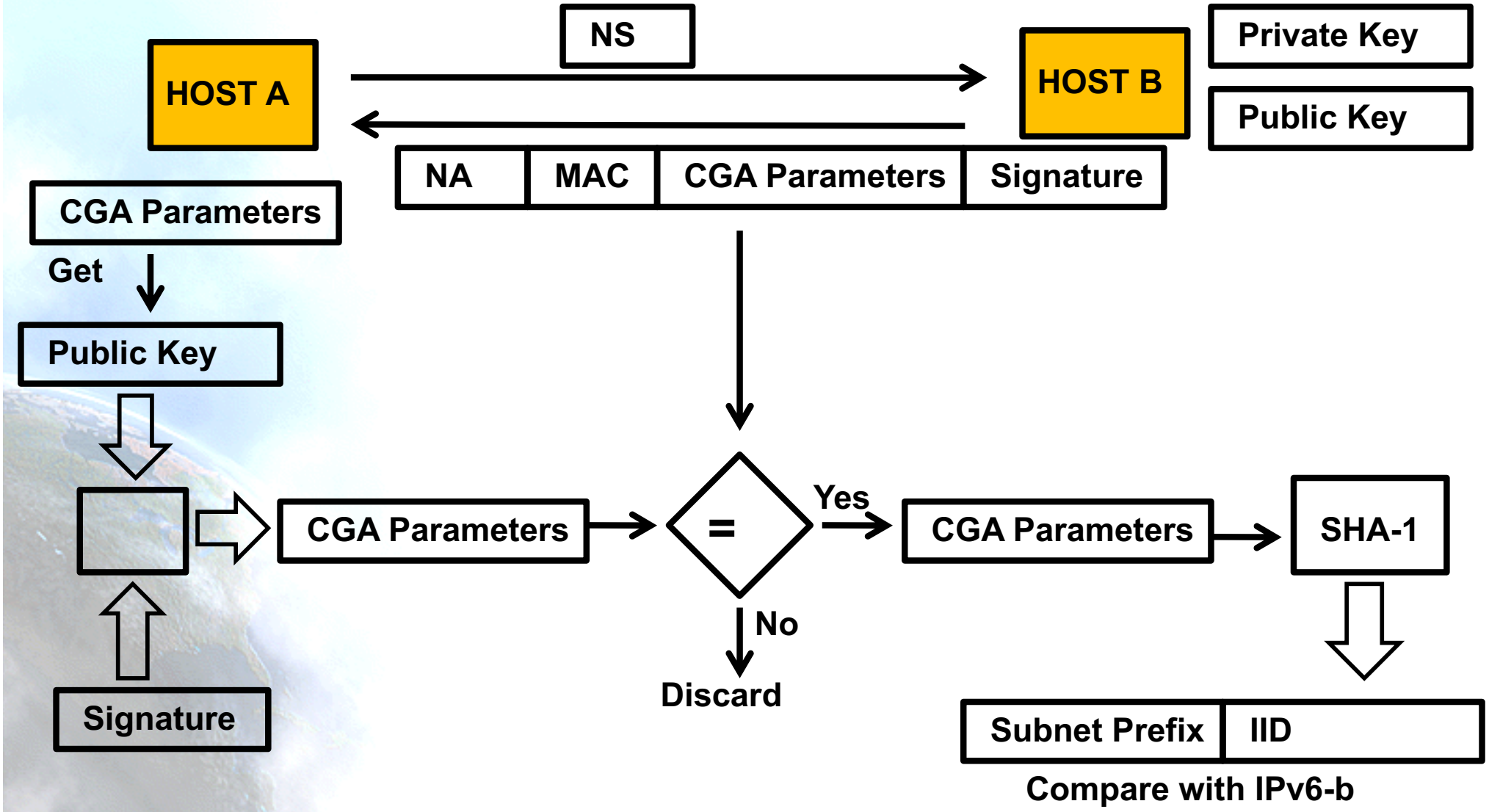
- An actual NDP message includes
  - an NDP message header
    - ICMPv6 header
    - ND message-specific data
  - and zero or more NDP options, which are formatted in the Type-Length-Value format



- To secure the NDP, a set of new Neighbor Discovery options is introduced and used to protect NDP messages
  - **CGA parameters:** Modifier, Subnet Prefix, Public Key
  - **Nonce:** Random number to protect against replay attacks
  - **Signature:** CGA parameters and nonce signed using a private key

How SEND works (1)

- Host A wants to know MAC of IPv6-b (host B) -> sends NS



How SEND works (2)

- RAs could be protected using somthing similar
- RAs are signed by routers, that need an X.509 certificate associated to their key pair in order the hosts trust on them
- X.509 certificate and the signature are included in all RAs
- Certificate is issued by an CA in which hosts should trust
- Two new ICMPv6 messages are created:
  - **CPS** (Certification Path Solicitation): Used by hosts to get router's certificate
  - **CPA** (Certification Path Advertisement): Answer from router containing its certificate

Distributed Security Model

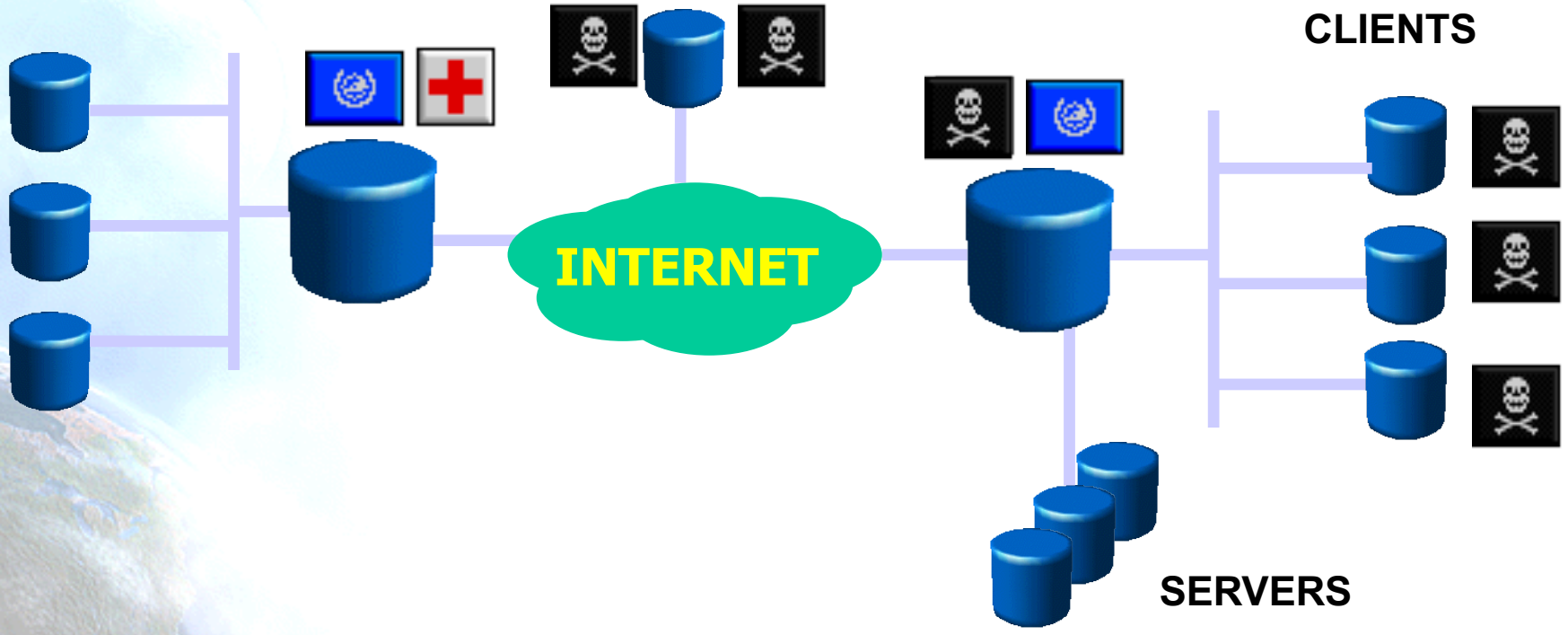
Overview

- In IPv4 the common practice is to use the **perimeter model**, when deploying security on networks. This model is based on isolating networks by means of security devices through which all traffic must pass through.
- Nowadays more and more security tools are being “moved” from network to hosts: firewalls, anti-virus, anti-spam, anti-malware, etc.
- This leads to the **distributed or end-host security model**. Where the security policy is enforced on the end-host. This fit much better with the end-to-end paradigm that IPv6 has brought back.
- Also it should be taken into account the “new” IP devices that will use IP networks to connect: PDAs, laptops, home automation, cell phones, etc. They all will need to be protected everywhere!

Deployment considerations

- The most common case when deploying IPv6 is to **add** IPv6 to the existing IPv4 network, resulting in a dual-stack network.
- This way we found the same perimeter security model and security devices to be used for IPv6 security. This could have some advantages for network staff and drawbacks in case of lack of IPv6 support.
- It is expected that in the (near-)future this will change because of the deployment of IPv6-only networks.

Perimeter Security Model (1)

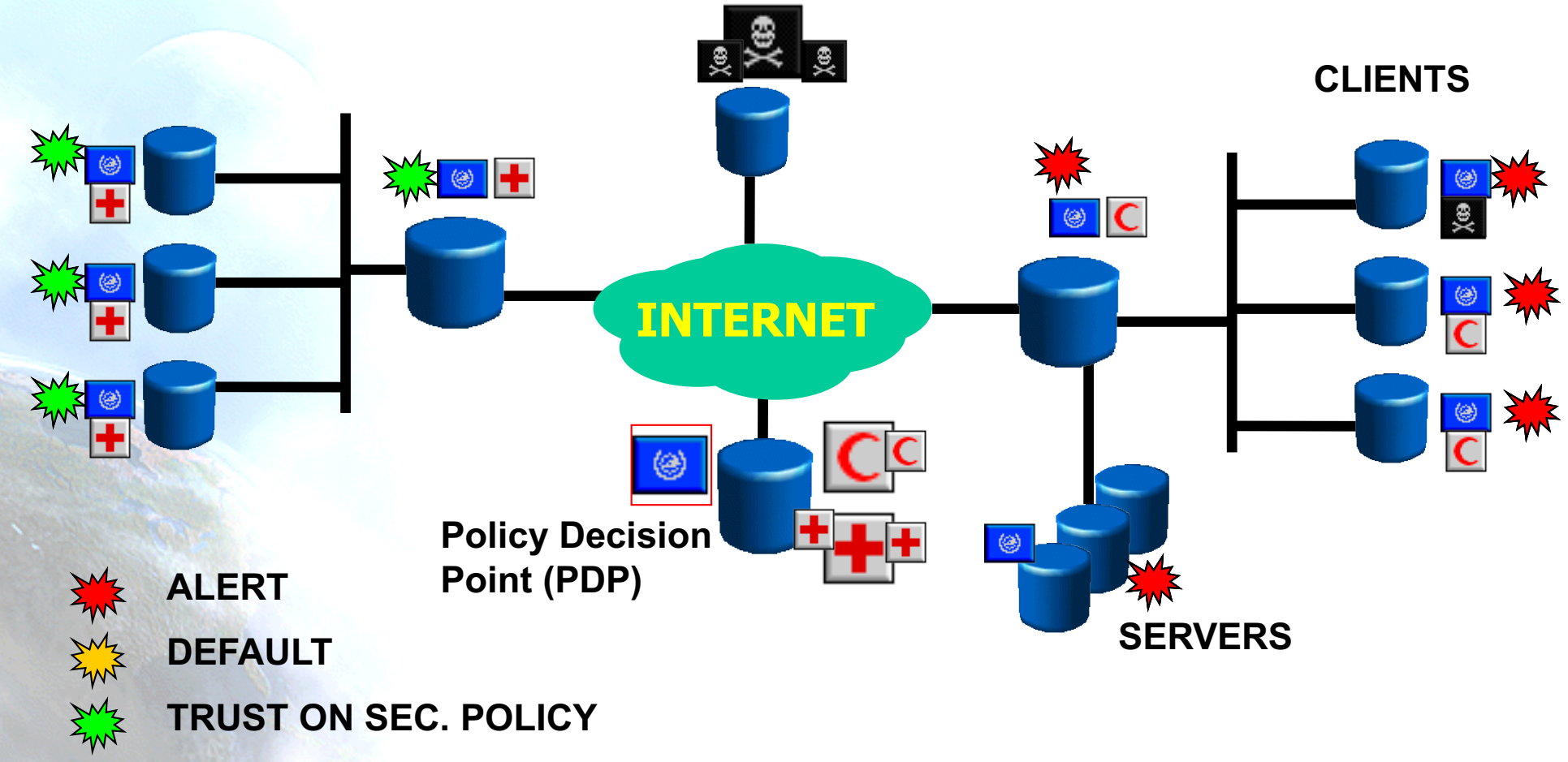


THREAT Sec. Policy 1 Sec. Policy 2 Policy Enforcement Point (PEP)

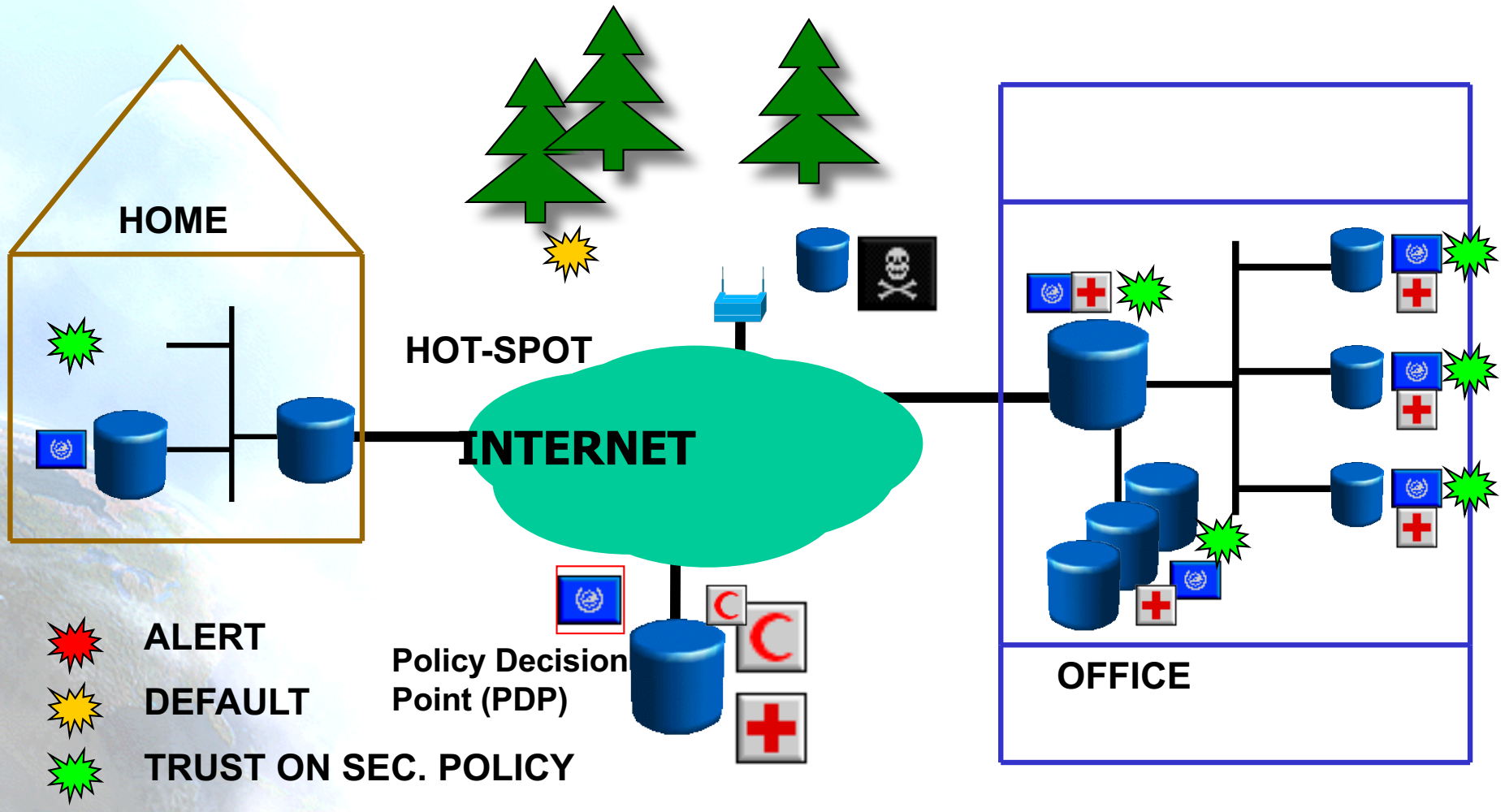
Perimeter Security Model (2)

- The security of a host **depends on the point of the network it is connected to**
- **Main Assumptions**:
  - Threats come form “outside”
  - Protected nodes won’t go “outside”
  - No backdoors (ADSL, WLAN, etc.)
- **Main Drawbacks**:
  - Firewall-dependant model
  - Do not address threats coming from inside
  - FWs usually act as NAT/Proxy
  - Special solutions are needed for Transport Mode Secured Communications

Distributed Security Model (1)



Distributed Security Model (2)



Distributed Security Model (3)

- **BASIC IDEA:** Security Policy centrally defined and distributed to PEPs. The network entities will authenticate themselves in order to be trusted
- **THREE elements**:
  - Policy Specification Language.
  - Policy Exchange Protocol.
  - Authentication of Entities.
- **Main Assumptions**:
  - Threats come from anywhere in the network
  - Each host can be uniquely and securely identified
  - Security could be applied in one or more of the following layers: network, transport and application

Distributed Security Model (4)

- **Main Drawbacks**:
  - Complexity
  - Uniqueness and secured identification of hosts is not trivial
  - Policy updates have to be accomplished in an efficient manner and assure the hosts follow these policies
  - A compromised host still is a problem
  - Is PDP dependant: more complexity to address this

Distributed Security Model (5)

- **Main Advantages**:
  - Flexibility in the definition of security policies
  - Protects against internal attacks
  - Doesn't depend on where the host is connected to
  - Still maintain the centralized control
  - Enables the end-2-end communication model, both secured or not
  - Better decision could be taken based on host-specific info
  - Enables a better collection of audit info
  - Can control the outgoing attempts from each host, avoiding local network misbehavior or malicious practices.
  - Enables distributed and cooperative security solutions

Distributed Security Model (6)

- There is some work that could fit into this model:
  1. **Cisco NAC** (Network Access Control): The host has to obtain network access by being complaint with a security policy.
  2. **Microsoft NAP** (Network Access Protection): create policies to validate computer health before allowing network access, update compliant computers and optionally confine non compliant computers to a restricted network.
  3. **Trusted Network Connect Work Group**: open architecture and a growing set of standards for endpoint integrity.
  4. **IETF NSIS WG**: It works in the direction of allowing the final host, previously authenticated, to open paths on firewalls.
  5. **IETF NEA WG**: Assess the "posture" of endpoint devices for the purposes of monitoring compliance to an organization's posture policy and optionally restricting access until the endpoint has been updated to satisfy the posture requirements.
  6. **IETF IDWG WG** (OLD): define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to management systems which may need to interact with them.

- The market and standards seems to go in the direction of end-host policy enforcement by means of network access control.

Thanks !

Contact:

- Jordi Palet: jordi.palet@theipv6company.com