

# Mitigating Security Risks in IPv6 Networks

Merike Kaeo

Double Shot Security

[merike@doubleshotsecurity.com](mailto:merike@doubleshotsecurity.com)

# Agenda

- Network Threat Model
  - Threat Actions (i.e. Attacks)
  - Threat Consequence
- IPv6 Security Considerations
  - Comparing IPv4 and IPv6 Security
- IPv6 Mitigation Techniques
  - Firewall Deployment
  - IPsec Deployment
  - Auditing

# Consider Attack Sources

- **Passive vs Active**
  - Writing and/or reading data on the network
- **On-Path vs Off-Path**
  - How easy is it to subvert network topology?
- **Insider or Outsider**
  - What is definition of perimeter?
- **Deliberate Attack vs Unintentional Event**
  - Configuration errors and software bugs are as harmful as a deliberate malicious network attack

# Passive vs Active Attacks

- Passive Attacks
  - Eavesdropping
  - Offline cryptographic attacks
- Active Attacks
  - Replay
  - Man-In-The-Middle
  - Message Insertion
  - Spoofing (device or user)
  - DoS
  - Protocol specific attacks

# Threat Consequences

- **Unauthorized Disclosure**
  - circumstance or event whereby entity gains access to data for which it is not authorized
- **Deception**
  - circumstance or event that may result in an authorized entity receiving false data and believing it to be true
- **Disruption**
  - circumstance or event that interrupts or prevents the correct operation of system services and functions
- **Usurpation**
  - circumstance or event that results in control of system services or functions by an unauthorized entity

# How Mitigate Most Threats?

- Secure end-system hosts
- Limit access to network
- Authenticate (device vs user)
- Based on claimed identity, allow (authorize) access to specific resources
- Audit network traffic
- Use confidentiality if needed

# Where Are Points of Vulnerability?

- Need to consider all devices attached to the network
  - Routers, switches, firewalls, hosts, servers
  - Cell phones, PDAs, IP phones
  - Printers, scanners
- Need to consider all paths someone can access the device
  - Physical
  - Logical
- Need to consider all points where data can be accessed
  - In transit
  - On a host, server, etc.

# Comparing IPv4 & IPv6 Security

- Fundamental issues are the same
  - Authentication
  - Authorization
  - Access control
  - Integrity
  - Confidentiality
  - Audit
- Difference arises from protocol variations

# IPv4 vs IPv6

Functionality	IPv4	IPv6
Addressing	32-bit, NAT	128-bit, Multiple Scopes
Neighbor Discovery	ARP	Auto Discovery
Autoconfiguration	DHCP	Serverless, Reconfiguration, DHCP
Routing	MD-5 Auth	IPsec protection
Security	IPsec added	IPsec part of packet

# Comparing Risk Mitigation:

- Reconnaissance
- Unauthorized Access
- Header Manipulation
- Fragmentation Attacks
- Layer 3 and 4 Spoofing
- ARP and DHCP attacks
- Broadcast Amplification
- Viruses and worms

# Reconnaissance

- IPv4
  - Tools widely available (NMAP, Nessus)
- IPv6
  - Ping sweep and port scans more difficult to complete
  - New multicast addresses simplify finding of key systems (routers, DNS servers, etc)

# 64 bit Subnet Scanning

- At 100M pings / second (40 Gbps fdx), it takes **> 5,800 years** to scan the address range for just one subnet.

*Worm and virus propagation will fail or will have to find an alternative search path.*

# Reconnaissance Protection for IPv6 Networks

- Use static address for internal communications that are MAC address based and pseudorandom address for traffic destined to Internet
- Filter internal use IPv6 addresses
- Use standard but non-obvious static addresses for critical systems

# Reconnaissance Protection for IPv6 Networks

- Filter unneeded services at the firewall
- Selectively filter ICMP
  - Neighbor discovery uses ICMP
  - Neighbor discovery - neighbor solicitation
  - Neighbor discovery - neighbor advertisement
  - Router advertisement and router solicitation if autoconfiguration is used
  - Fragmentation is only done on end station which requires path maximum-transmission-unit discovery
- Maintain host and application security

# Unauthorized Access

- IPv4
  - Usually single address per interface
- IPv6
  - IPv6 node can have multiple addresses
  - Significance varies
    - Local subnet (link local FE80::/10)
    - Organization (site local FC00::/16)
    - Internet (global unicast addresses)

# Unauthorized Access Protection

- Limit access to IPv6 end nodes through combination of addressing and routing
- Potentially easier in IPv6 due to address scoping
- Check out address allocations from [www.ripe.net/ipv6/ipv6allocs.html](http://www.ripe.net/ipv6/ipv6allocs.html)

# Header Manipulation

- IPv4
  - Option Headers
- IPv6
  - Extension headers
    - Possible circumvention
      - All v6 endpoints are required to accept packets with a routing header
      - Host may accept and process routing header so the routing header can be used to circumvent security policy at firewalls
    - Mitigation
      - Designate specific set of hosts for MIPv6 operation
      - Validate operating systems to ensure end systems do not forward packets with routing header
      - Filter on routing header to drop packets

# Comparing ICMP v4/v6 Filters Through Firewall

Description	IPv4	IPv6
Echo Request	Type 11	Type 128
Echo Reply	Type 0	Type 129
Destination unreachable	Type 3 / Code 0	Type 1 / Code 0
Fragmentation needed but DF bit set	Type 3 / Code 4	N/A
Time exceeded	Type 11	Type 3

# Additional v6 ICMP Considerations

Type	Description	Justification
2	Packet too big	For correct operation of PMTUD
4	Parameter problem	Cannot process packet because cannot identify a field in a header or the packet itself
130-132	Multicast listener	Routing device must accept these messages to participate in multicast routing
133	Router solicitation	Needed for IPv6 autoconfiguration
134	Router advertisement	Needed for IPv6 autoconfiguration
135	Neighbor solicitation	Duplicate address detection and Layer2 (MAC) -to-IPv6 address resolution
136	Neighbor advertisement	Duplicate address detection and Layer2 (MAC) -to-IPv6 address resolution

# Filtering Considerations

- Multicast
  - Permit link-local multicast address to firewall to provide neighbor discovery
  - Layer 3 firewalls should never forward link-layer multicast addresses
  - Filter any packets with multicast source address
- Should support traffic filtering based on
  - source and destination addresses
  - IPv6 option headers
  - upper-layer protocol type information

# Fragmentation Overlap

- **Description**

- reassembly algorithms result in new fragments overwriting any overlapped portions of previously-received fragments

- **Exploit**

- an attacker could construct a series of packets in which the lowest (zero-offset) fragment would contain innocuous data (and thereby be passed by packet filters), and in which some subsequent packet having a non-zero offset would overlap TCP header information and cause it to be modified. The second packet would be passed through most filter implementations because it does not have a zero fragment offset.

# Fragmentation Overlap Example

1. The filter is configured to drop TCP connection request packets.
2. The first fragment contains values, e.g., SYN=0, ACK=1, that enable it to pass through the filter unharmed.
3. The second fragment, with a fragment offset of eight octets, contains TCP Flags that differ from those given in the first fragment, e.g., SYN=1, ACK=0.
4. Since this second fragment is not a 0-offset fragment, it will not be checked, and it, too will pass through the filter.
5. The receiving host, if it conforms fully to the algorithms given in [RFC 791](#), will reconstitute the packet as a connection request because the "bad" data arrived later.

# Tiny Fragments

- Description
  - it is possible to impose an unusually small fragment size on outgoing packets.
- Exploit
  - If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter

# Tiny Fragment Example

- The first fragment contains only eight octets of data (the minimum fragment size).
- In the case of TCP, this is sufficient to contain the source and destination port numbers, but it will force the TCP flags field into the second fragment.
- Filters that attempt to drop connection requests (TCP datagrams with  $SYN=1$  and  $ACK=0$ ) will be unable to test these flags in the first octet, and will typically ignore them in subsequent fragments.

# IPv6 Fragmentation

- Fragmentation prohibited by intermediary devices
- Overlapping fragments not allowed
- Drop fragments less than 1280 min MTU
- Multiple extension headers make following policy rules more difficult when passing fragments

Result: IPv6 Provides BETTER Fragmentation  
Attack Mitigation

# IPv6 Fragmentation Protection

- Deny IPv6 fragments to an infrastructure device
- Fragment reassembly capability
  - If first fragment does not include layer 4 header (due to multiple extension headers), packets may need to be reassembled

# Address and Port Spoofing

- RFC 2827 ingress filtering to prevent layer 3 address spoofing at the origin
- Addresses which have not yet been allocated
- Addresses which are reserved
- IPv6 addresses are set up for easy summarization
- IPv6 has potentially more addresses to spoof
- Tunneling mechanisms allow for hard to trace source but that is true for v4 and v6
- Make sure outer v4 source matches address embedded in the v6 source to achieve better traceback

# Mitigating Spoofing Attacks

- Reality Check: Spoofing will exist
- Can reduce risk by combining security measures
  - Use ingress/egress filtering
  - Correlate IP and MAC address
  - Cryptographic protection

# ARP and DHCP

- IPv4
  - many tools to deal with ARP and DHCP spoofing
- IPv6
  - Neighbor Discovery
- Issues
  - Stateless autoconfiguration messages can be spoofed
  - Router and neighbor solicitation and advertisement messages can be spoofed and will overwrite existing neighbor-discovery cache information on a device
- Mitigation
  - Use static neighbor entries for critical systems until ability to detect misuse of neighbor discovery messages or to secure their transport

# Routing

- IPv4 routing can be protected using MD-5
  - Not scalable
  - Re-keying issue
  - Could use IPsec with IKE but if making change then preference is to upgrade to IPv6 as well
- IPv6 routing can be protected using IPsec
  - Scalable
  - Better re-keying
- Routing Filters
- TTL Check

# Broadcast Amplification

- Example: ping echo request results in response flood
- IPv4 mitigation with no directed broadcast
- IPv6 REMOVES the concept of dedicated broadcast from the protocol and specific language used to mitigate these types of attacks
  - RFC2463 “ICMPv6 messages should not be generated as a response to a packet with an IPv6 multicast destination address, a link-layer multicast address or a link-layer broadcast address.”
- Filter on ingress multicast source address

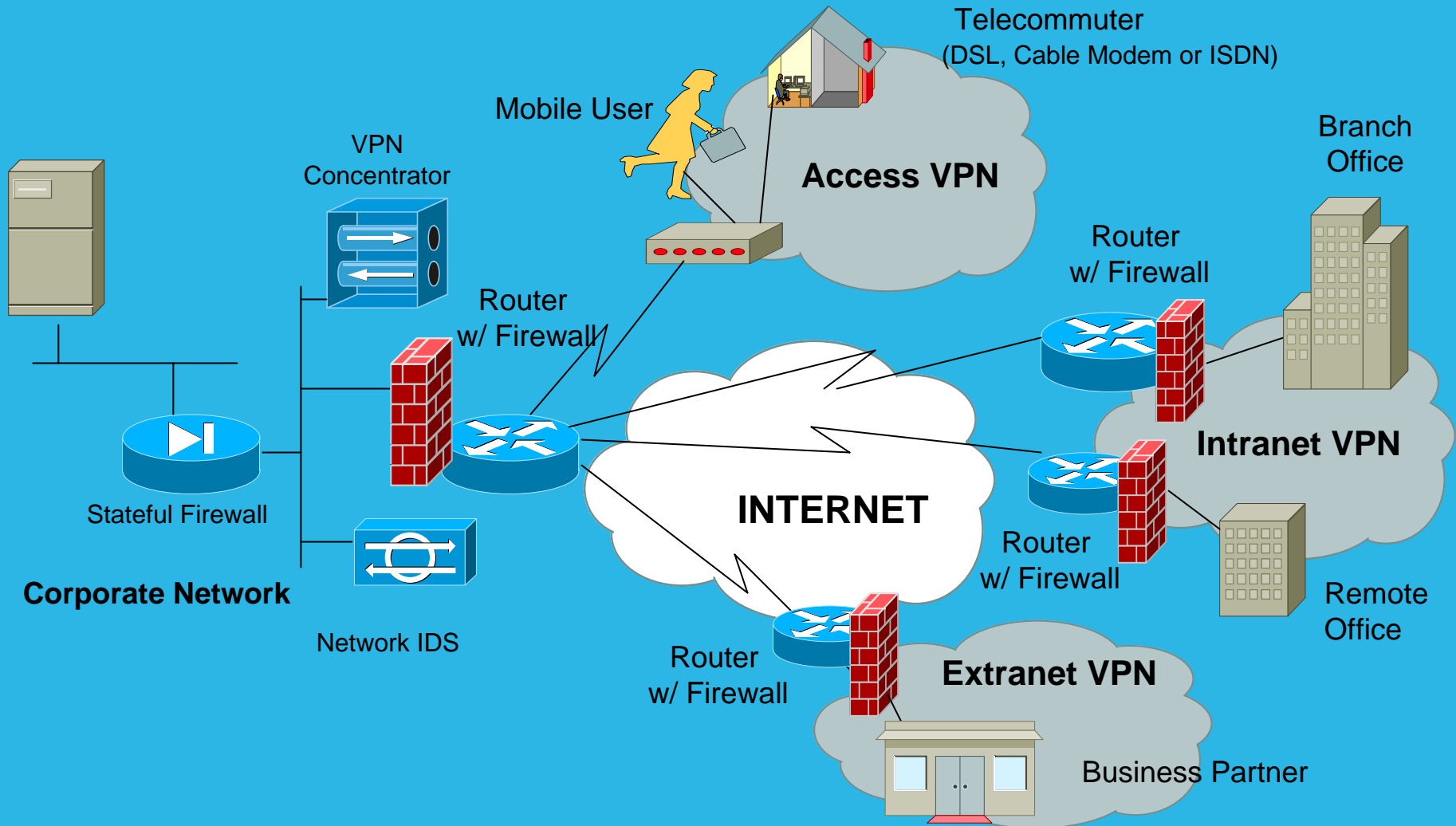
# IPv4 vs IPv6 Security Summary

- IPv4 and IPv6 have very similar security issues
  - [www.cisco.com/security\\_services/ciag/documents/v6-v4-threats.pdf](http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf)
- Many attacks are EASIER to mitigate in the IPv6 environment
  - Security was part of groundwork architecture
- Start implementing IPv6 solutions to understand the different security considerations
  - Easier to implement end-to-end security

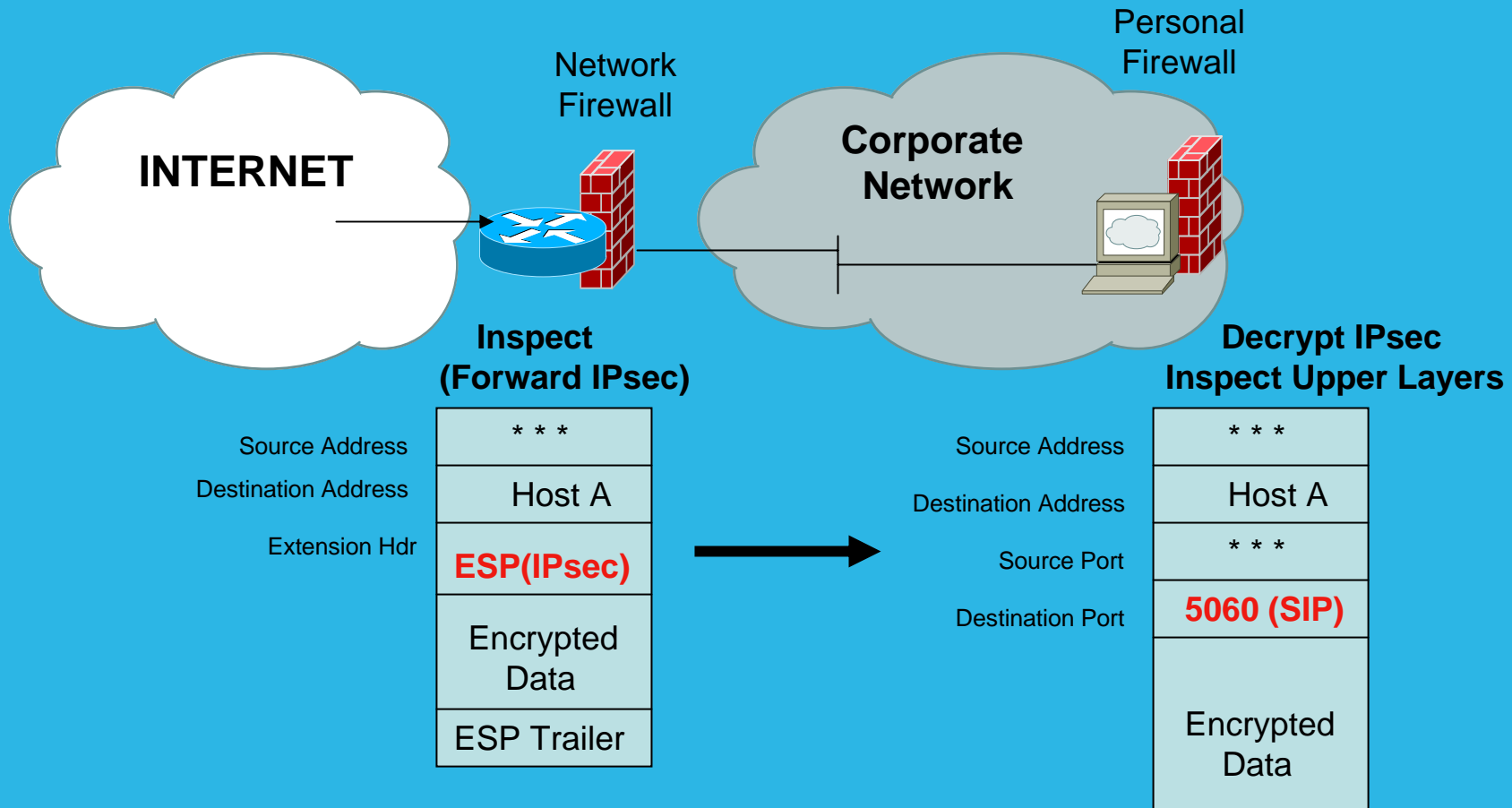
# IPv6 Mitigation Techniques

- Firewalls
  - Where is the perimeter?
  - Limitations when using IPsec
- IPsec
  - AH & ESP with NULL Encryption
  - ESP
- Auditing

# Firewall Deployment



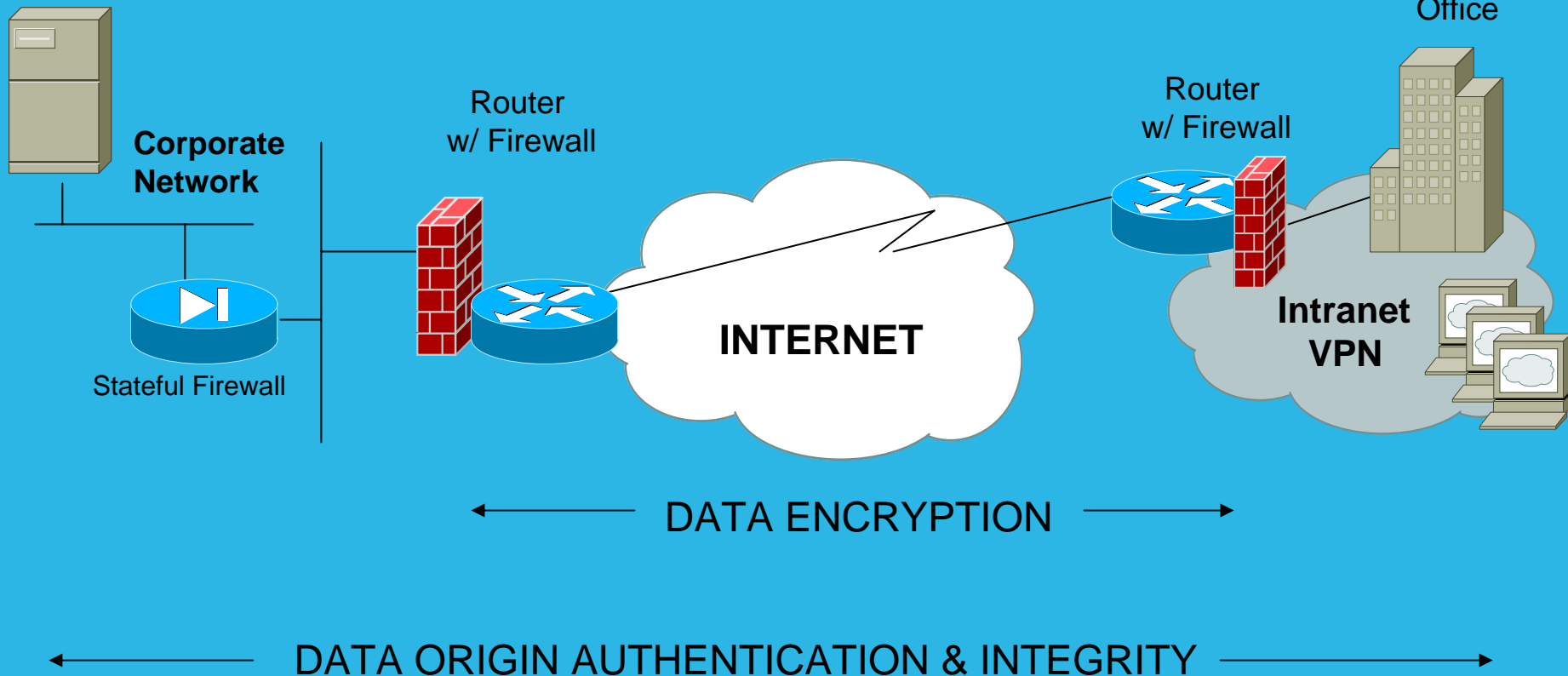
# Coordinated Firewalls



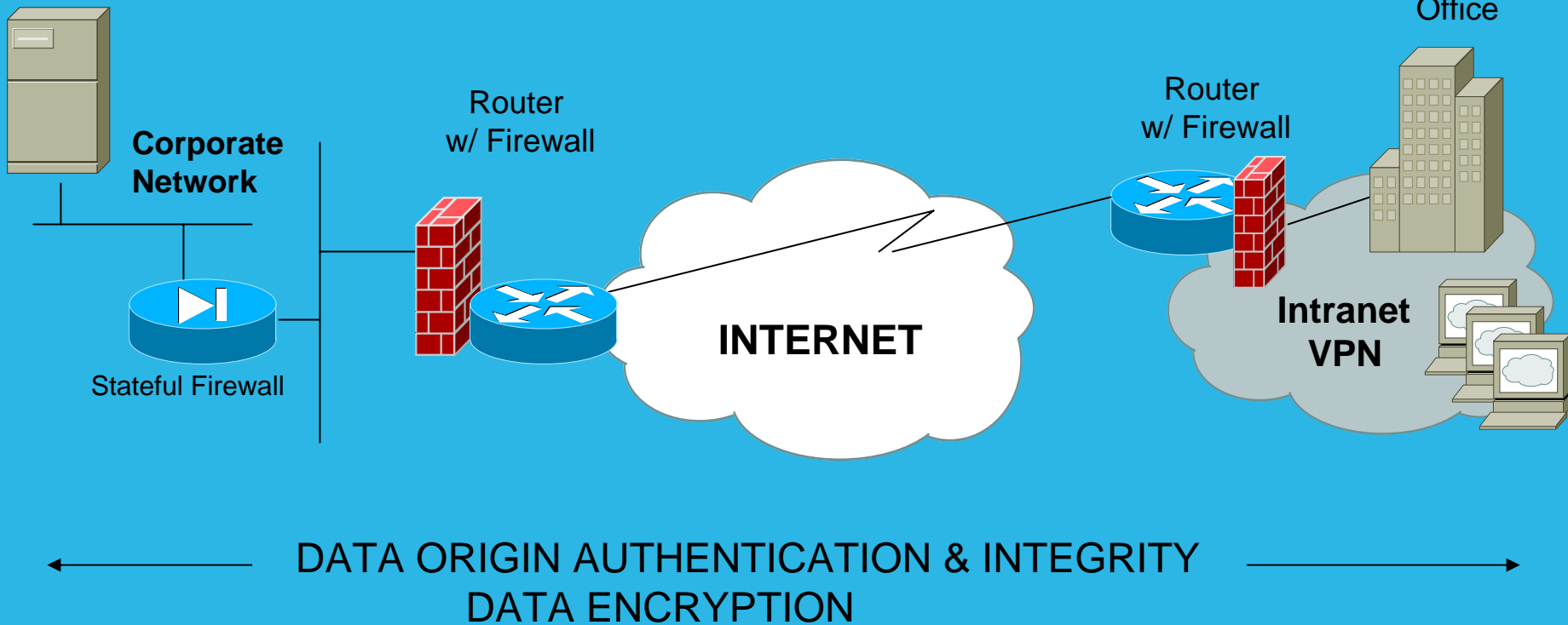
# IPsec Myth

- Deploying IPsec does not always mean that packets are encrypted end-to-end.
- IPsec can be used end-to-end for:
  - Data origin authentication and integrity
  - Data origin authentication and integrity and encryption

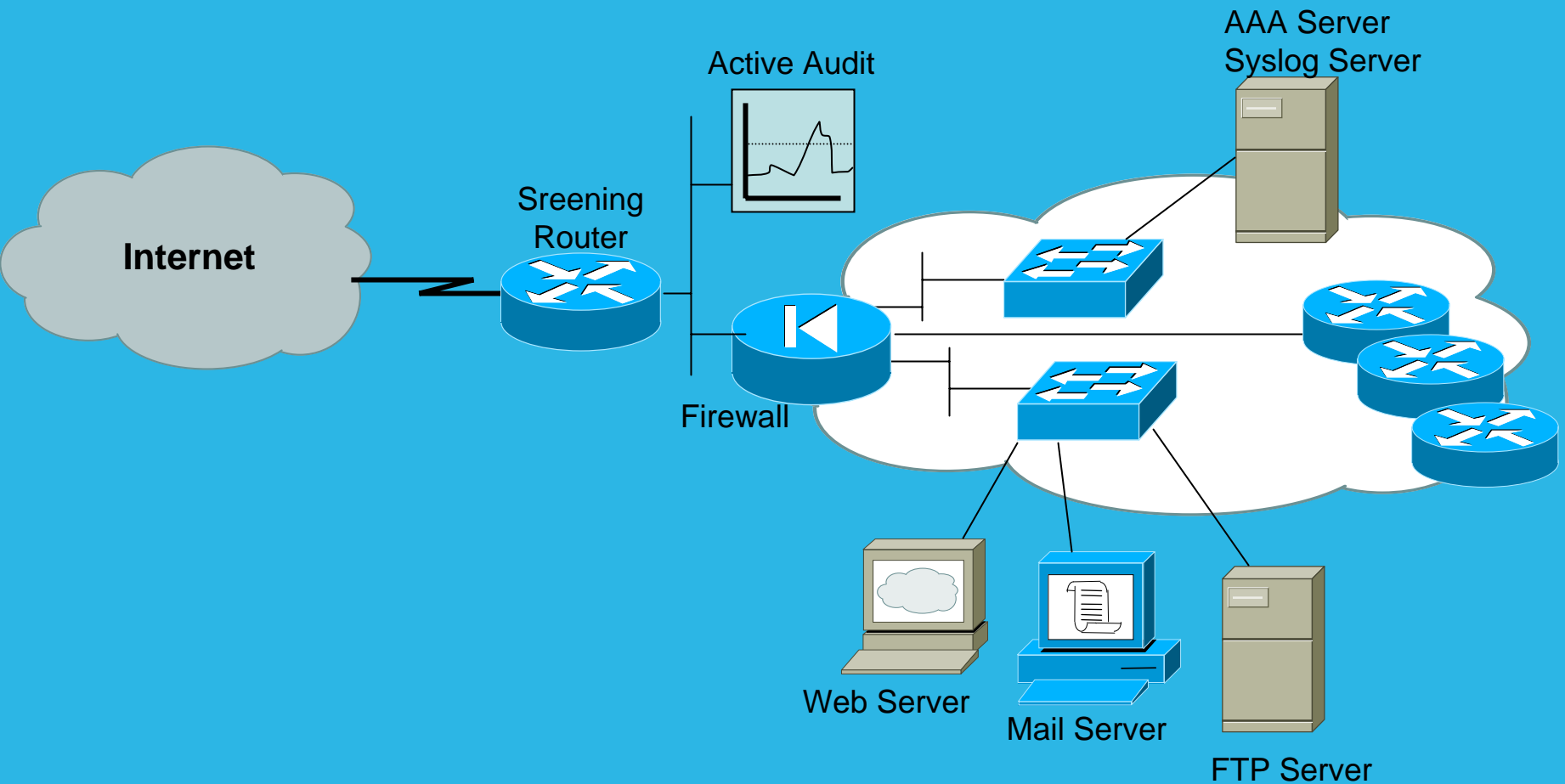
# IPsec and IPv6 (Intermediary Encryption)



# IPsec and IPv6 (End-To-End Encryption)



# IPv6 Auditing (Where and What)



# QUESTIONS ?