CCIE Security Version 5
Advanced Technologies Class

Copyright © www.ine.com

Virtual Fragmentation Reassembly

What is Virtual Fragmentation Reassembly - VFR?

How can it defend against fragmentation attacks?

Copyright © www.ine.com

VFR Overview

- What is VFR?
  - VFR allows a router to virtually reassemble the fragments of an IPv4/IPv6 packet
- What is the scope of this technology?
  - Security reasons, stopping fragmentation attacks
  - Functional reasons, used by stateful firewalls and NAT64 for example

Copyright © www.ine.com

VFR Overview

- What fragmentation attacks can it detect and block?
  - Tiny fragmentation attack
  - Overlapping fragment attack
  - Buffer overflow attack

Copyright © www.ine.com

VFR Overview

How does VFR work?

- The router waits for all fragments in order to rebuild the initial IP packet
- The router reassembles the packet and performs necessary actions, like NAT
- The router drops the reassembled packet
- The router forwards further the IP fragments

Copyright © www.ine.com

Virtual Fragmentation Reassembly

- IOS implementation steps
  - Enable VFR for IPv4 and/or IPv6 at the interface level
  - When enabled, specify direction, default being inbound
  - Verify its functionality
- To protect the router, additional options are available
  - Maximum number of fragments per datagram
  - Maximum time for waiting all fragments of a datagram
  - Maximum number of concurrent reassemblies

Copyright © www.ine.com

Copyright © www.ine.com