
# IPSec and Firewalls

Ivan W. Wallis
Security Applications Engineer
SSH Communications Security, Inc.

March 5, 2001

# Agenda

- The Role of VPN Gateways and Firewalls
- Internet Firewalls
- Integrated VPN/Firewall Architectures
- Implementation Decisions
- Conclusion

# The Role of VPN Gateways and Firewalls?

- VPN devices provide end-to-end secure and authenticated traffic
- Firewalls define rules for inbound/outbound network traffic
- Integration provides centralized policy management

# Internet Firewalls

- Traditional packet filtering (1G)
- Proxies and Gateways (2G)
- Packet Inspection (SMLI, 3G)
- Next generation VPN/Firewall Security Gateways (4G)
- Advantages/Disadvantages of each

# Traditional Packet Filtering (1G)

- Uses network-layer rules to filter in/out going packets
- Filtering by:
  - Origin and destination addresses
  - Protocols (TCP or UDP)
  - Port numbers
- Inadequate for environments requiring more detailed analysis of upper-layer protocols (i.e. proxy servers)

# Proxies and Gateways (2G)

- Inspect 2 layers of the IP packet
- Provides more rigorous filtering
- Ability to customize filter schemas
  - Example: filter specific user accounts or shell commands within FTP
- Usually associated with a performance penalty (requires additional processing for application-layer protocols)

# Packet Inspection (3G)

- Commonly referred as Stateful Inspection or Stateful Multi-Layer Inspection (SMLI)
- Uses similar approach to 2nd Generation Firewalls
- Packet inspection uses “snap shots” of data to determine the necessary action
- Traffic screening algorithms examine each packet and compare against known states
- Provides Inspection over Interpretation
- Result is improved data throughput

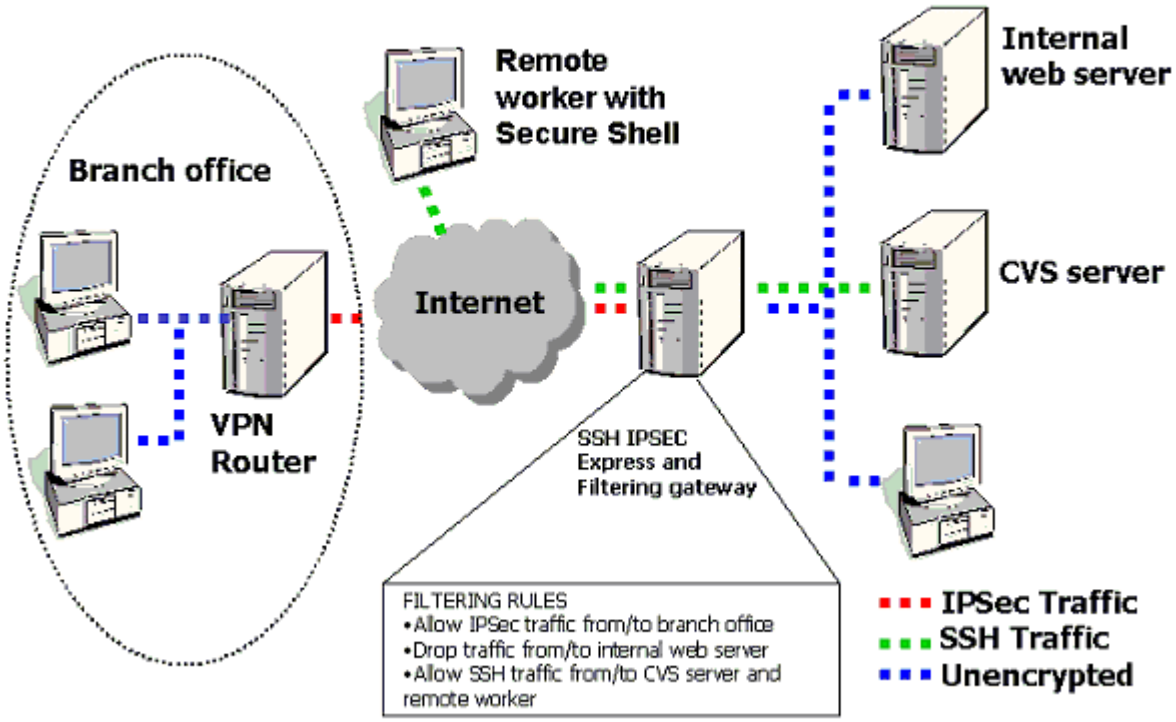
# Why VPN/Firewall SG's

- Advantageous to combine VPN gateways and firewalls
  - Common security policies
  - Modularized
  - Architecture stresses secure as well as accessible services
- Packet filtering provides basic framework for integrating IPSec modules

# Next Generation VPN/Firewall Security Gateways (4G)

- Provides hook for complementing VPN traffic
- Allows additional filtering on inbound and outbound data
- Integrated network access control
- More importantly:
  - Allows for custom stateful inspection software
  - Control over packet “states”
  - Integrated authentication schemes
- Defines Traffic Profiling to maintain connection states for all network data

# Example Scenario




- Allow secure IPSec traffic from/to branch office
- Apply post-filtering rules to data exiting the VPN tunnel (e.g. allow SSH traffic from/to CVS Server and remote device

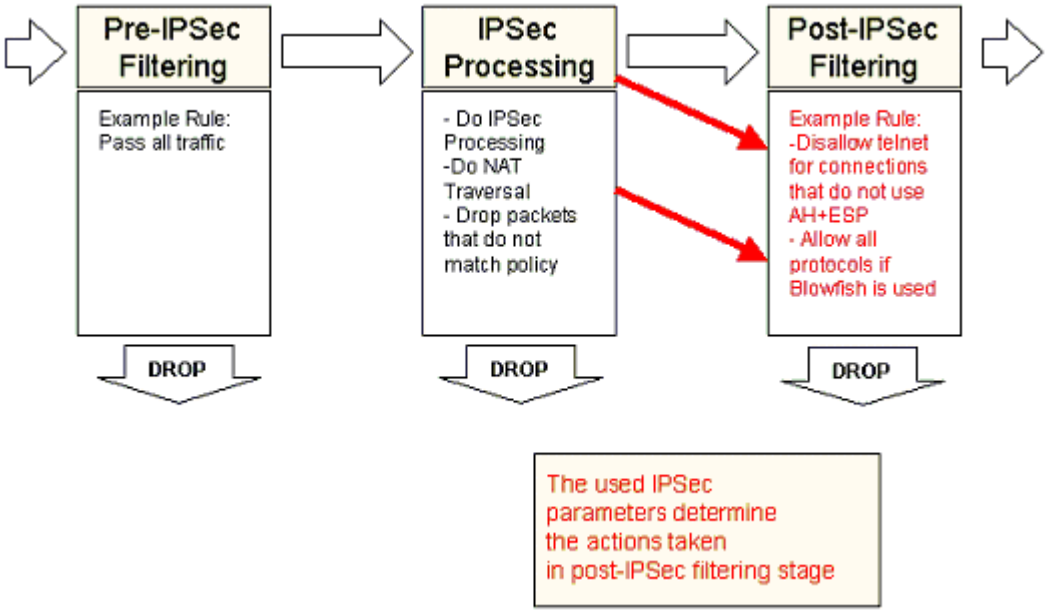
# Integrated VPN/Firewall Architectures

- Different configurations
  - Integrated
  - VPN in front of Firewall
  - VPN behind Firewall
  - VPN and Firewall in parallel
- Consider:
  - Threats
  - Access control of VPN traffic
  - Centralized management
  - Scalability
  - Integrated user authentication

# Implementation Decisions

- Extend the simple packet filtering architecture
  - The need for “state” processing
- Add custom packet inspection software (SMLI)
  - Provides a modular approach in defining how network traffic should be analyzed
  - Example:
    - A Stateful Inspection Module can be integrated to perform analysis on SNMP transactions
- Define pre-IPSec and post-IPSec filtering rules
  - Allow/deny certain packets before passing onto next stage
  - IPSec packets most likely would be processed through post-filtering rules
- Define/refine how VPN and Firewall processes interact

# Example: Filtering Event Chain




- A generic event chain for VPN traffic
- Traffic profiling results from combining pre-post filtering rules with IPSec connections
- State management is key

# Filtering Event Chain

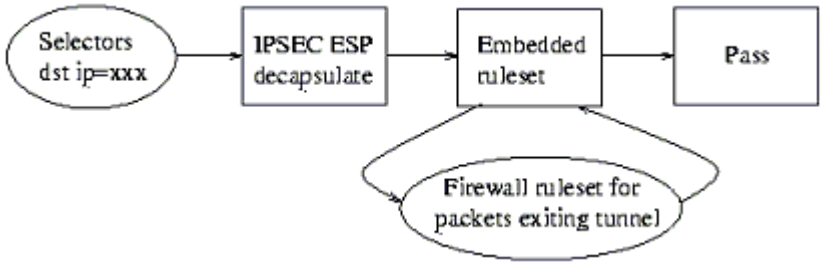
- Pre-filtering
  - Typical Firewall role
  - Allow/deny packets based on simplistic access control and packet filtering

    e.g. Allow IPSec traffic to be passed to IPSec engine
- IPSec processing
  - Typical VPN role
  - NAT traversal
  - Drop packets that do not match a particular security policy

    e.g. Disallow telnet connections that do not use ESP
- Post-filtering
  - Also a firewall role
  - Match connection state for more granular filtering

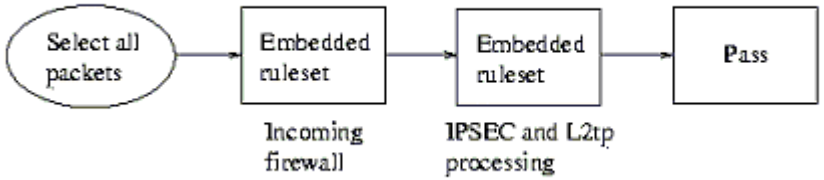
    e.g. Perform additional firewall rules on data exiting the IPSec process

# Packet Processing in Stages




- Activate Firewall ruleset on packets exiting tunnel
- Allows for more refined filtering

# Packet Processing in Stages (Cont.)




- Apply rules to packets entering the Firewall
- Pass this state onto next stage for IPSec and L2TP processing
- Apply firewall action to packets exiting the IPSec processing stage

# Conclusion

- Advantageous to combine VPN gateways and firewalls:
  - IPSec security parameters can be used as filtering criteria
  - Common security policies
  - Modularized (use existing framework)
  - Architecture stresses secure as well as control over accessible services
  - Common management
- Packet filtering provides basic framework for integrating IPSec modules

# Questions

- Any questions?

# Thank you!

- Presentation available on Connectathon web site (www.connectathon.org)
- White papers available at http://www.ssh.com/tech/whitepapers
- Making the Internet Secure
  - SSH Secure Shell
  - SSH IPSec Express Toolkit
  - SSH NAT-T
  - SSH Sentinel
  - SSH Certifier