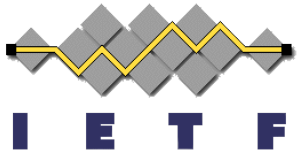
draft-baker-opsawg-firewalls

Fred Baker



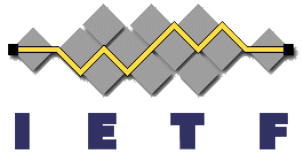
Purpose of this draft

- We have had discussions in v6ops and (now) in Homenet regarding firewalls
  - RFC 6092 “Simple Security”
  - draft-vyncke-advanced-ipv6-security
- I personally don’t think they have been very productive, and think the community needs to have a less emotional discussion on the topic
  - Firewalls are a market requirement, but for bad reasons
  - There are strong feelings about firewalls pro and con, and the discussions tend to not be helpful.

Draft discussion

- Introduction
- Common kinds of firewalls
  - Perimeter security: Protection from aliens and intruders
  - Pervasive access control
  - Intrusion Management: Contract and Reputation filters
- Reasoning about Firewalls
  - The End-to-End Principle
  - Building a communication
  - The middle way
- Recommendations

Perimeter security: Protection from aliens and intruders

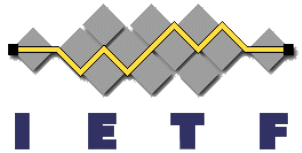


- In Cisco equipment, we call this a “context-based” or “zone-based” defense.
  - There is a “protected region” and “everywhere else”
  - Sessions may originate from the “protected” region
  - No sessions, or only certain sessions, may originate from “outside”
- Primary comment:
  - “I want my NAT for security” presumes this model
  - It’s actually a weak defense model, and disrupts certain service models
  - PCP and UPnP are protocol models for allowing sessions into the domain for services

Pervasive access control

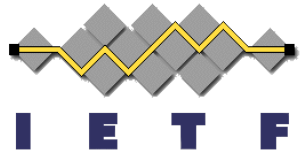
- So-called “role-based” access control
  - Systems organized into groups for security management
  - Policy applied in network that
    - Permits communication within a group
    - Permits communication between stated pairs of groups
    - Excludes or limits all else
  - One group is “everyone else”
- More flexible, but still has impact on service deployment
  - Requires an IT department to manage

Intrusion Management: Contract and Reputation filters



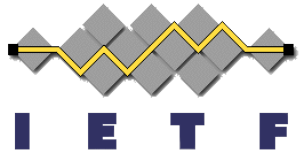
- Generally implemented as
  - Access control lists,
  - Anomaly-based intrusion management,
  - Signature-based intrusion management, or
  - Reputation-based systems
- Basic policy: allow communication barring a specific reason not to
- Weakness:
  - That's not how we raise our children
  - People often fail to maintain such software on hosts…

Reasoning about firewalls, part 1



- I conclude that a firewall protects two things
  - Protection against some forms of infrastructure attacks
  - Second layer of defense for attacks on hosts
  - Hosts still must be their own primary defense
- There may be better approaches to infrastructure defense
  - Passive IP Addresses, for example

Reasoning about firewalls, part 2



- Poorly-implemented firewalls make it difficult to deploy new technologies or services
  - Explicit Congestion Notification
  - SCTP
  - …

Recommendations: ZBAC

- IF someone implements zone-based access control
  - It SHOULD be possible for a host to assert that it is willing to field incoming traffic for a class of application
  - Firewall SHOULD exclude traffic that nobody explicitly wants

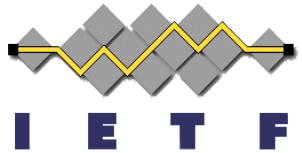
Recommendations: RBAC

- Observation: this requires active policy management anyway
- It's better to implement using the control plane (routing) than the data plane (filtering)
  - Make the policy systemic if possible – if Alice should not talk with Bob, Alice should not have a route to Bob.

Recommendations: Active policy algorithms

- Reputation, Anomaly, and Signature models require regular and frequent updates
  - Do so (duh)
  - May not fit residential market

General observations



- Middleware should not prevent innovation
  - Prevent what is known to be bad
  - Don’t prevent the unknown; it might be good
- Making assumptions about address spaces is also less than useful
  - In IPv4, we have a lot of experience with the evils of NAT
  - In IPv6, there can also be issues in coupling between address domains.
  - So don’t make assumptions you can’t immediately justify

Way forward this draft

- What I have said in this draft…
  - Seems patently obvious to me.
  - Seems controversial to others; we spend a lot of time, and waste energy, debating it.
  - Is it useful to say?
  - Would folks like to debate?