

BOF: IETF OPSEC WG Current Operator Practices & Packet Filtering Capabilities

Ross Callon
Engineer

Distinguished



Agenda

- Brief Status of OPSEC WG (Ross Callon)
 - What we are doing
 - Why we are here
 - Why you should care
 - Question: What's missing?
- Current Operator Practices (Merike Kaeo)
- Packet Filtering Capabilities (Chris Morrow)



IETF OPSEC WG

- Initial seed: UUnet internal document
 - Documented security requirements
 - Brought to IETF
- Result
 - RFC 3871 (Operational Security Reqts...)
 - IETF OPsec Working group
 - We are producing series of BCPs
 - Define router (& switch) capabilities needed to allow networks to be operated securely



Why We Are Here

- Two of our documents are ready for working group last call
- We are here to solicit additional input from network operators
- Input can be
 - Given to authors here and now
 - Sent to authors via email
 - Sent to WG email exploder



Why Should You Care?

- To motivate / educate vendors
- To motivate / educate your management
 - If you know it needs to be done, and its in a BCP, then you might get them to let you do it
- To motivate / educate peer networks
 - Their security problems are your problems
 - (it is easier to help us now, than to help them later)



The Documents

- Operational Security Current Practices
 - draft-ietf-opsec-current-practices-03
 - What is actually being done wrt security?
- Filtering Capabilities for IP Network Infrastructure
 - draft-ietf-opsec-filter-caps-01
 - What packet filtering capabilities are needed, in detail



What's Missing??

- What operational security issues are you seeing that need to be addressed in standards?
 - What capabilities are important, but aren't being covered by our existing work?
 - Are additional BCPs needed?

