DC Security and Availability (some thoughts)

Joel Jaeggli
For
Afnog 2011

Mentality

- Security and availability considerations are not an after-thought or something that you can readily bolt on to already deployed services
  - Sometimes you have to take on such problems when you inherit someone else's mess
- Rather it's a set of practices and posture applied to the design, development, deployment, operation, and terminal phases of an application's lifecycle.

Goals

- The goals are:
  1) Document it like it's going to be run and diagnosed by someone whose never seen it before.
  2) Limit the exposure of a service to the component's necessary to use it.
  3) Allow the rapid and consistent deployment of new services using standardized procedures
  4) Leverage best common practices, from industry and community sources.
  5) Deliver solutions that will continue to scale with growth.

Goal 1

- Document like it's going to be run by someone else
  - Deploy a wiki, doesn't matter which one, use it.
  - Document port mappings
  - Rack elevations
  - Circuit labels
  - Host functionionality
  - Contact information
  - Service ownership
  - Make a runbook

Goal 1 - 2

- People move on.
- You hire new people.
- You want take a vacation or come to Afnog.

Goal 2

- Limit the exposure of services
  - A web server shouldn't be listening on any other ports externally.
  - Segregate internal and external networks
  - Don't inadvertently expose services that are necessary to the external network (if your recursive resolver is required, don't put it out there)
  - Seperate mangement from production.
  - Transparently in the forwarding plane makes debuging much simpler (please don't drop ICMP)

Goal 3

- Rapid and consistent deployment of new services
  - A service has an owner
  - Owner is responsible for the documentation package necessary to deploy and operate a service
  - Deployment divided into phases
    - Development
    - Deployment
    - Production
  - Common infrastructure elements have documented owners responsible for providing them
    - Might include ip addresses, rack elevations, switch ports, load balancer vips etc.
  - Consider taking an ITIL class

Goal 4

- Leverage Best Common practices
  - Participate in communities of interest related to your activities (mailing lists)
  - Participate in regional user groups (LUGS) most likely and organizations like Afnog
  - Get your employees training.
  - Consult and be aware of IETF BCP where appropiate.
  - Beware “experts”, “trade rags”, and “vendors”. journalists paid speakers and your sales guy do not operate networks or internet services.

Goal 5

- Deliver scalable solutions.
  - Plan for growth
  - Gold plated solutions to problems are frequently too expensive to repeat.
  - A service that is scaling well costs less to operate on a per user basis as the the user base grows.
  - Silos create duplication which is waste.
  - Beware designs that result on the creation of multiple overlapping network technologies (e.g. fibe channel) rather than one. Two networks are always more expensive than one.

Some things you may have heard

1) “You need a firewall”
2) “Defense in Depth is the best strategy”
3) “Drop all ICMP”
4) “NAT adds security”
5) “We're aiming for 99.999% uptime”

You Need a Firewall?

- Providing internet services means that by default all connections are unsolicited. (not much point in stateful inspection if you're going to accept them all)
- In the face a DOS attack or high connection load the firewall is the most fragile network element and the first to fail.
- Outgoing connections from private addresses need to be natted, vpn tunnels need to be terminated so you're not going to get away entirely without them

Defense in Depth is the best strategy?

- Defense in depth is a military strategy by which overlapping layers of security buy time for penetration to be detected and responded to
- The analogy can only be casually applied to network security.
- Duplicating functionality is expensive and leads to confusion as whom is responsible for what.
- What you should do
  - Consolidate indentity credentials into AAA systems
  - Compartimentalize access based on groups
  - Restrict direct connections to management network, operation should be via bastion hosts

Drop All ICMP?

- Dropping all ICMP means:
  - Path-mtu discovery is broken
  - Ping no longer works
  - You need these, so do your customers.
- You can safely drop some ICMP e.g. fragments
- You can rate limit ICMP to reduce DOS risk...
- Transparency of the fowarding plane both inside and outside datacenter is of enourmous utility when you're trying to figure out what's wrong with your network.

NAT adds security?

- The only security benefit associated with Network address translation from private addresses is that it's hard to map incoming connections to internal addresses (your Load balancer is probably doing DNAT).
- When you build networks with private addresses it's rather hard to tell if you're leaking traffic (everyone else uses the same prefixes)
- NAT is a tool, it is not a security feature.

We're aiming for 99.999% uptime?

- 5 9's is 5.26 minutes of downtime a year.
  - It's unrealistic (e.g. needlessly costly) not to mention infeasible under most circumstances.
- What is realistic, is to track and measure the duration of any outages you encounter.
- Calculate actual availability
- Set targets potentially with room for improvement.
- Identify and work on problem areas.

Extras

Log monitoring Tools

- Loganalyzer
  - http://loganalyzer.adiscon.com/
- Splunk
  - http://www.splunk.com/
- Sawmill
  - http://www.sawmill.net/