ISD–SSL
The best SSL appliance in the world

By
Claes Wikstrom, Tony Rogvall and Johan Bevemyr
{klacke,tony,jb}@bluetail.com

Alteon WebSystems
A Nortel Networks Company

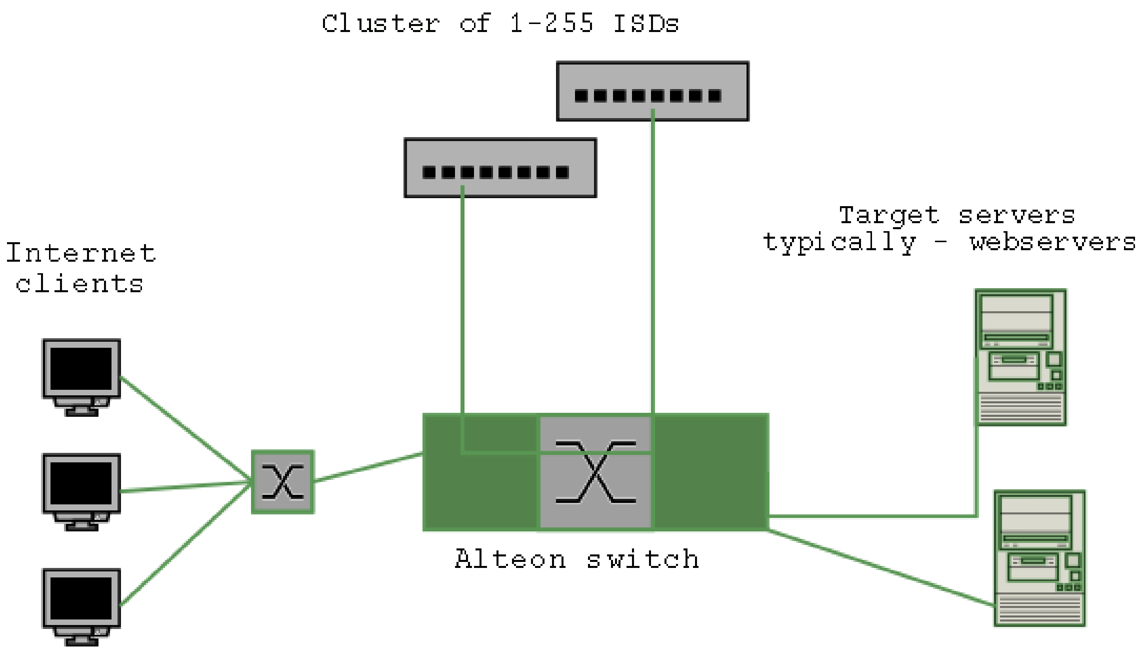
What have we built

- The ISD–SSL – An SSL terminating appliance (built in Stockholm)
- ISD–Core Platform – A general purpose platform intended to build Internet appliances with. (Stockholm)
- ISD–Tungsten – A superfast Checkpoint based firewall (San Jose)

ISD–Core platform

- A standard stackable 1U Dell PC with regular PCI slots, IDE disc and NICs
- Linux – stripped and rewritten /etc/rc structure
- Erlang, Mnesia
- The registry – up/down gradability of config data, semantic checks etc
- SSI – Single system image
- CLI – general purpose CLI engine
- Software managemnet, multiple Oses/applications, alarms logs events system management etc
- C api

Typical setup



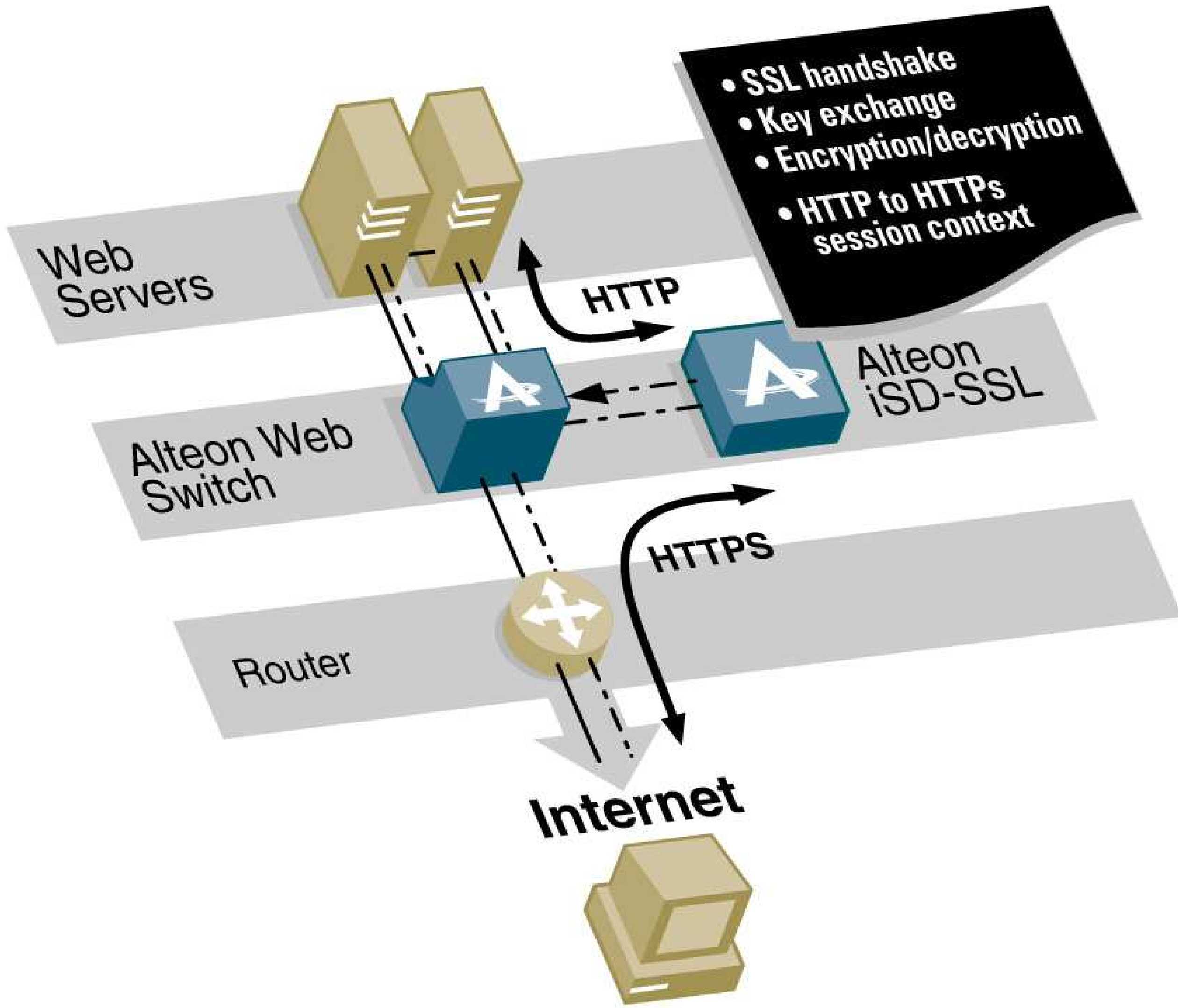
What is that Alteon switch anyway

- An L7 high speed switch
- HTTP, WAP, RTSP, ... aware switching
- A load balancer
- Hardware assisted high level switching and loadbalancing
- Typically sits in front of large web farms
- Pretty expensive piece of hardware

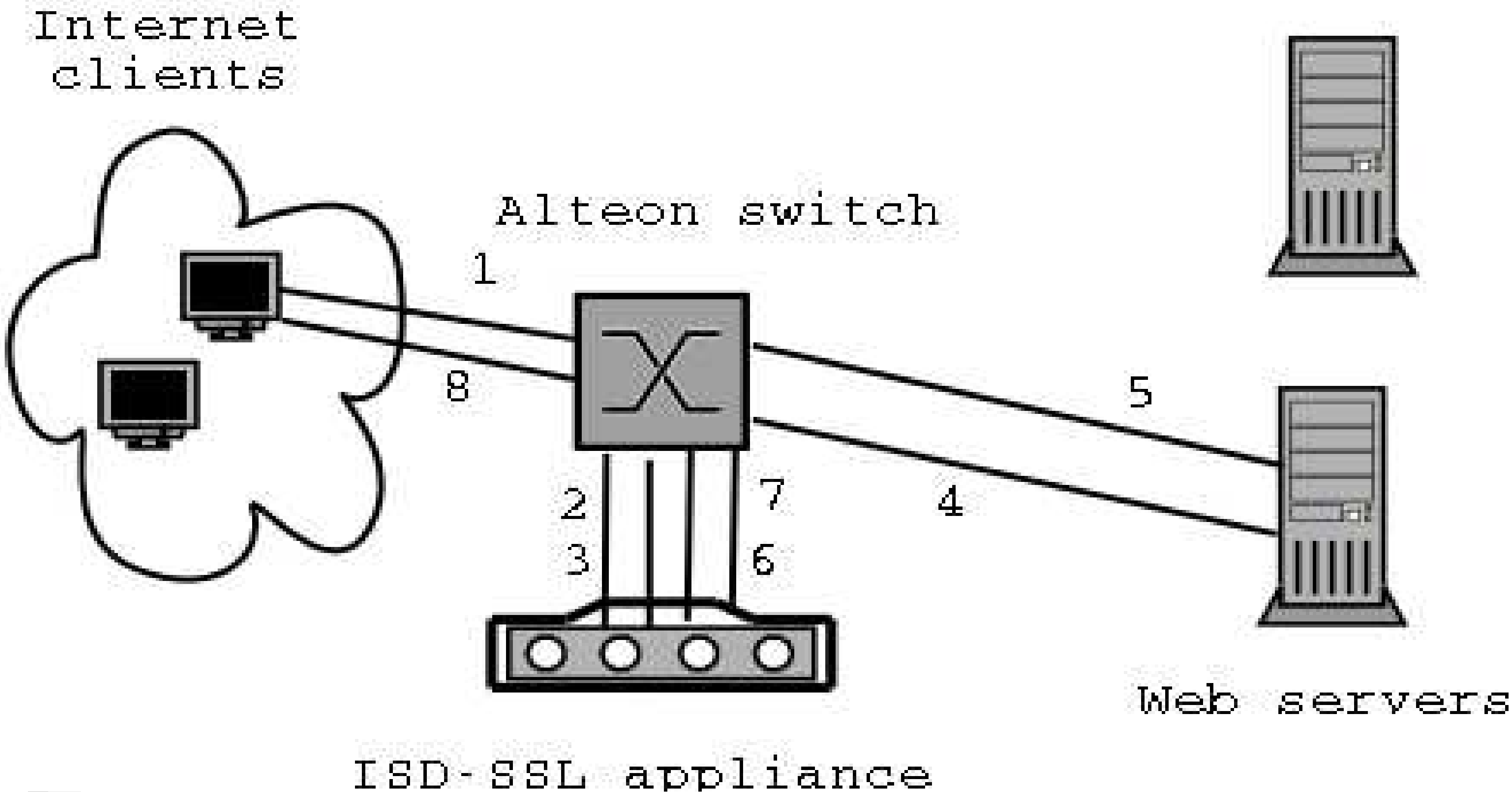
ISD–Core platform gives

- Scalability
- Fault tolerance
- CLI
- OS
- Hardware box
- Configuration

ISD–SSL



• SSL handshake
• Key exchange
• Encryption/decryption
• HTTP to HTTPs session context
Web Servers
HTTP
Alteon iSD-SSL
Alteon Web Switch
HTTPS
Router
Internet



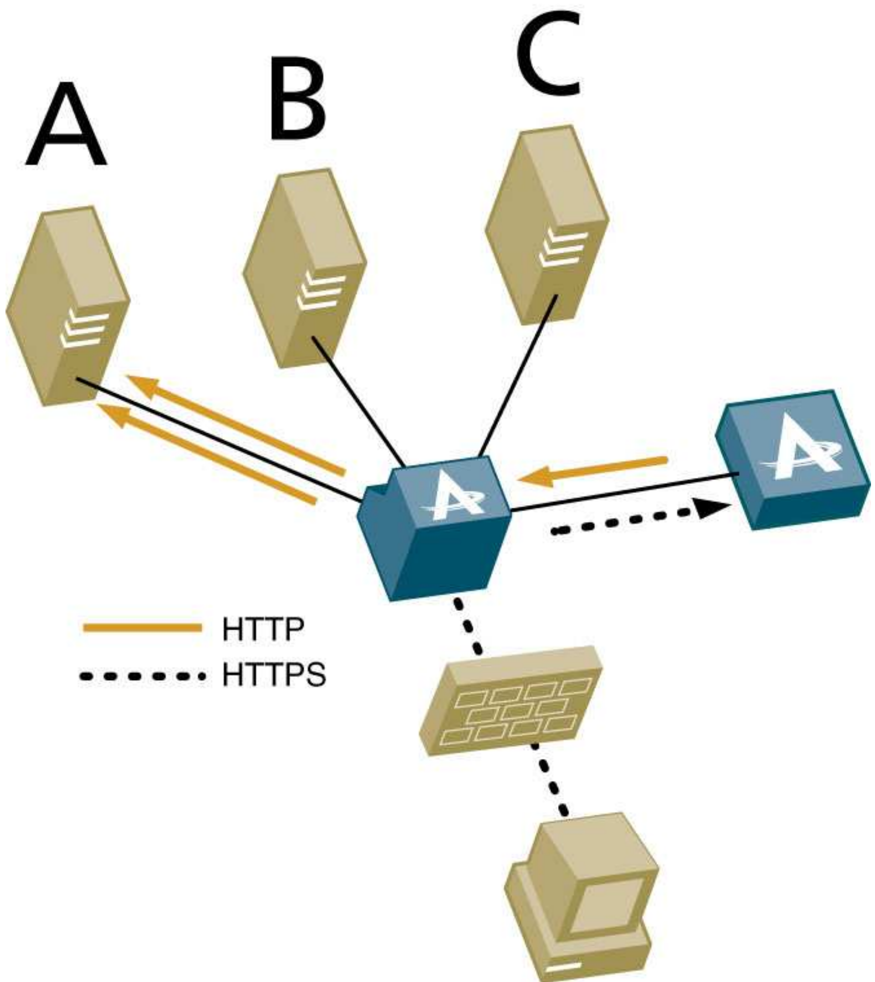
1. Switch redirects and loadbalances SSL traffic to group of ISDSSL boxes
2. ISD terminates SSL session.
3. ISD sets up a new connection to VIP:80
4. Switch load balances clear text traffic to group of webservers
5,6. Outbound traffic from webservers is once again redirected to group of ISDs
7,8 ISD proxies traffic. Encrypted SSL traffic on the client side, and clear text traffic on the servers ide

ISD–SSL feature set

- Easy certificate and key management
- Secure storage of private keys
- Scalable solution – buy more boxes and get more performance
- Hardware HA solution.
- SSL to the client, yet the switch sees clear text traffic and can do it’s funky L7 stuff with the traffic
- Offload webserver from RSA and bulk encryption
- Transparent – webservers see real client IP as source IP
- Client authentication, revokation lists
- Based on openssl + bignum hw cards

Shopping Cart Persistence – (uhh)

Without Manual Server Configurations



- iSD–SSL makes encrypted cookie visible to Web switch
- Web switch can associate shopping cart (HTTP) and payment (HTTPS) sessions from same user (cookie)
- User cookie is the most accurate persistence indicator
  - Due to mega– and micro–proxies

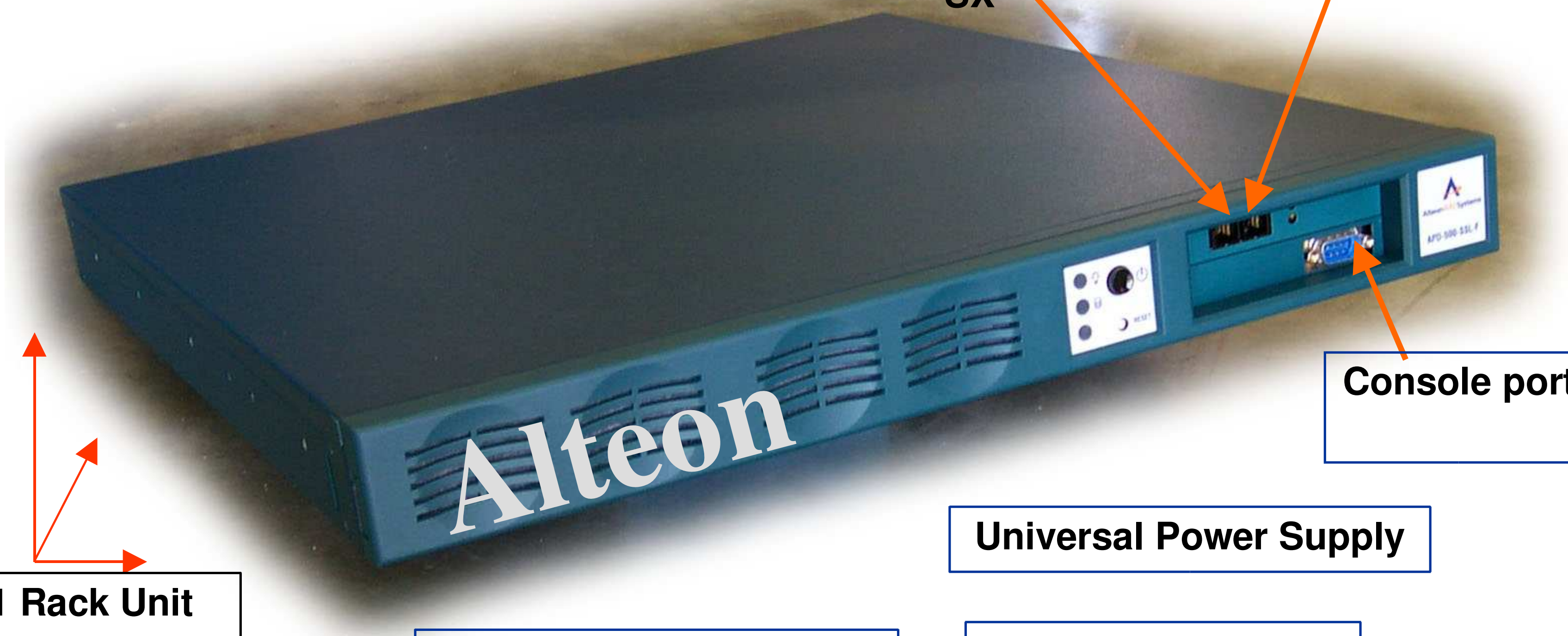
The BOX

A purpose–built appliance for processing SSL sessions

SC connector for 1000Base–SX

OR

2 RJ 45 connectors for 10/100Base–TX



Console port

1 Rack Unit

Universal Power Supply

1 SSL accelerator cards of 600 tps

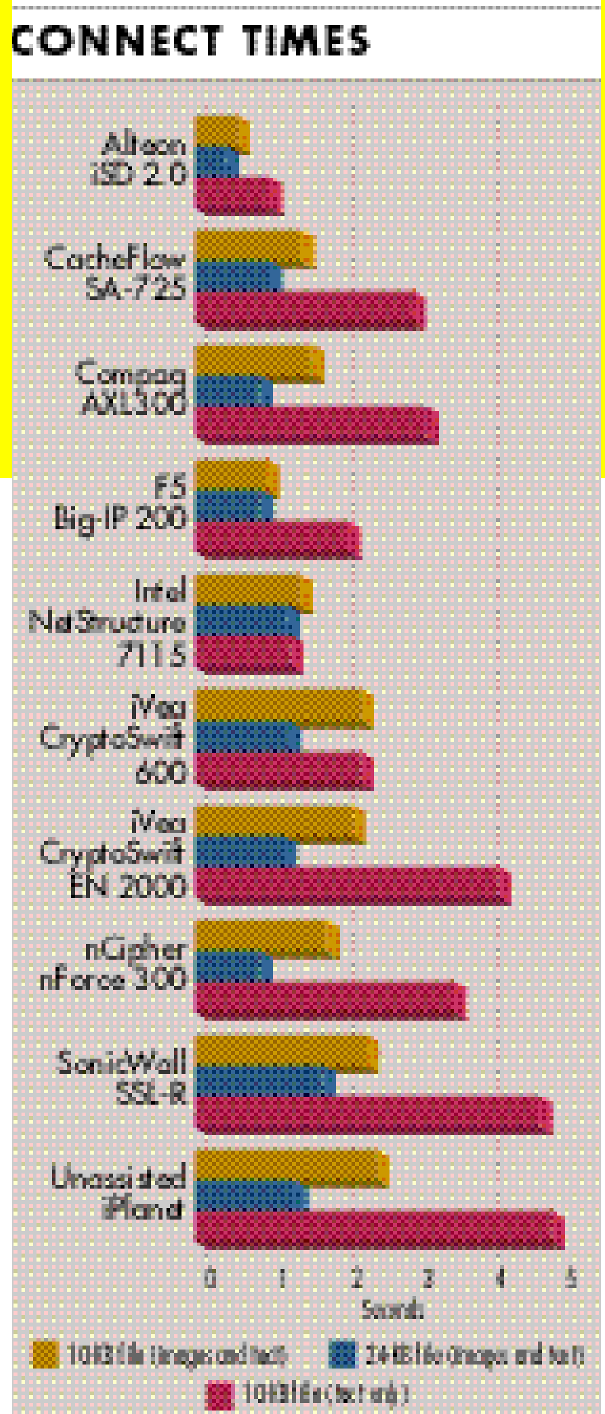
18 Gb hard disk

We are best, says
Network Computing magazine

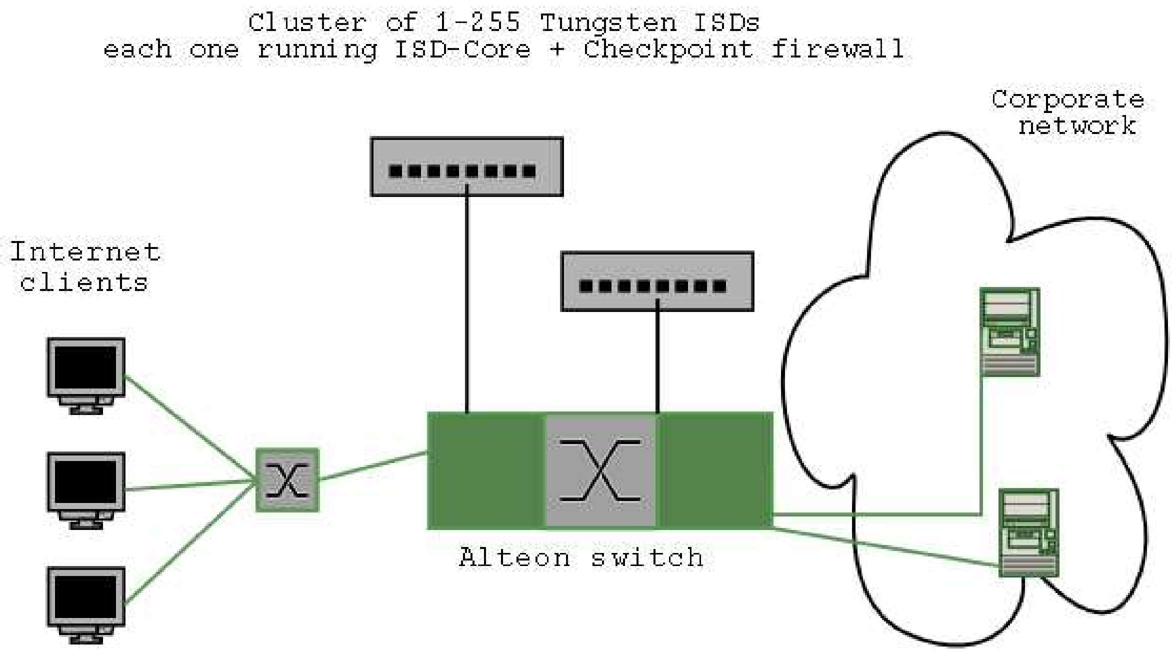
REPORT CARD ◆ External SSL Accelerators

	Weight	Alteon WebSystems iSD 2.0 SSL Accelerator	F5 Networks Big-IP 200 e-Commerce Controller 3.3.1	CacheFlow Server Accelerator 725	Intel NetStructure 7115 e-Commerce Accelerator	SonicWall SSL Accelerator—Rack Mount
SCALABILITY	25%	5	5	4	4	4
SECURITY	25%	4	4	4	4	4
PERFORMANCE	20%	5	4.5	4	3	4
CRYPTOGRAPHIC SUPPORT	10%	5	5	3	5	3
MANAGEMENT/CONFIGURATION	10%	4.5	4	4	3	3.5
PRICING	10%	4	3.5	3	4	3
TOTAL SCORE		**4.60**	**4.40**	**3.80**	**3.80**	**3.75**
		A	**A-**	**B**	**B**	**B**

A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5 A-C grades include + or − in their ranges. Total scores and weighted scores are based on a scale of 0-5. Customize the results of this Report Card to your environment using the Interactive Report Card®, a Java applet on Network Computing Online, at *www.networkcomputing.com*.



Tungsten Firewall



•SYN packet arrives at the switch (FIN or RST as well)
•Switch redirects packet to one of the ISDs
•Checkpoint software at the ISD decides what to do with that particular TCP flow
•ISD instructs switch that {src ip, src port, dest ip, dst port} shall be cut–through inside the switch
•FIN or RST arrives at the switch – switch redirects to the same ISD that got the SYN
•ISD terminates that TCP particular TCP flow

Customers

- Nokia
- Speedy tomato
- VMdata
- IRS (US tax department)
- Reuters
- Pentagon
- Zurich Insurance
- Chrysler   ... and lots lots more