



UPGRADING YOUR FIREWALL? IT'S TIME FOR AN INLINE SECURITY FABRIC

Badhrinarayanan Srinivasan
Manager, System Engineering



ATTACKS CONTINUE TO RISE

106 / hour

Average number of malware hits¹

66%

Growth in information-based security incidents from 2014 to 2015²

25%

Chance that your organization will be breached over next 24 months³

\$550k

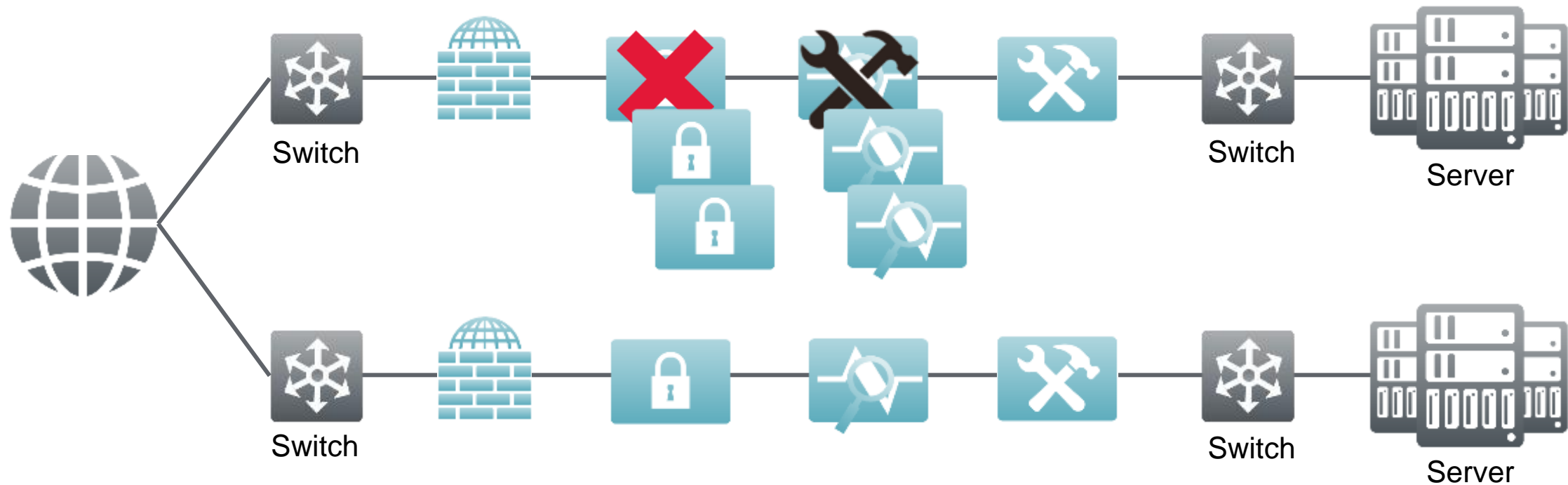
Average cost of unplanned outage for enterprises, growing 15% annually²

¹ ZK Research Study for Ixia, April 2016

² Kaspersky Lab, Cost of Security Breaches, September 2015

³ Ponemon Institute, Data Breach Study, May 2015

INLINE SECURITY IS EXPANDING

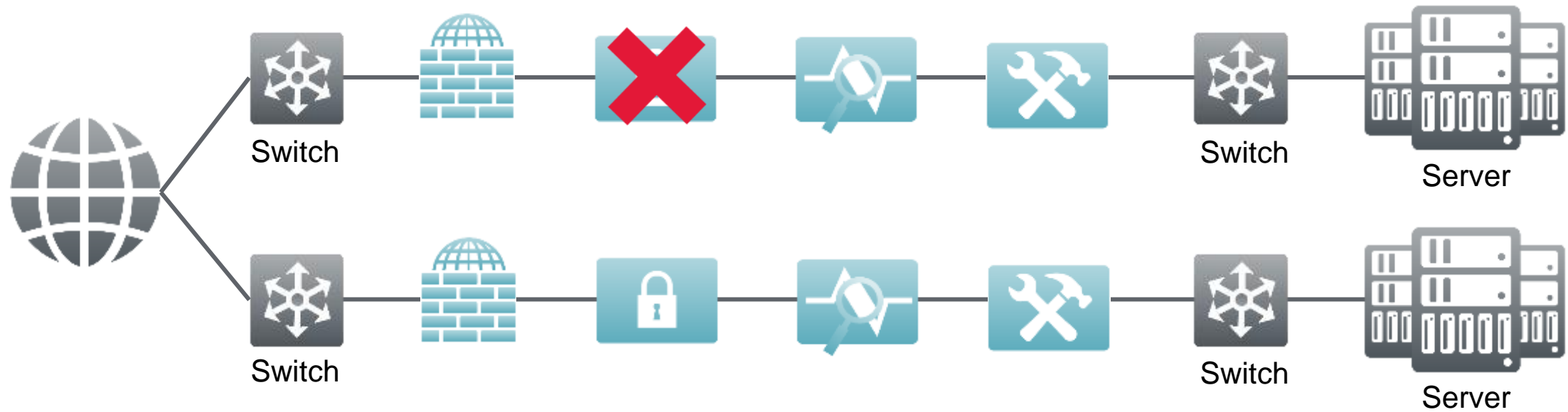


- Single points of failure
- Administrative tension
- Tools not used efficiently
- Difficult to scale

DISADVANTAGES OF CURRENT PRACTICES

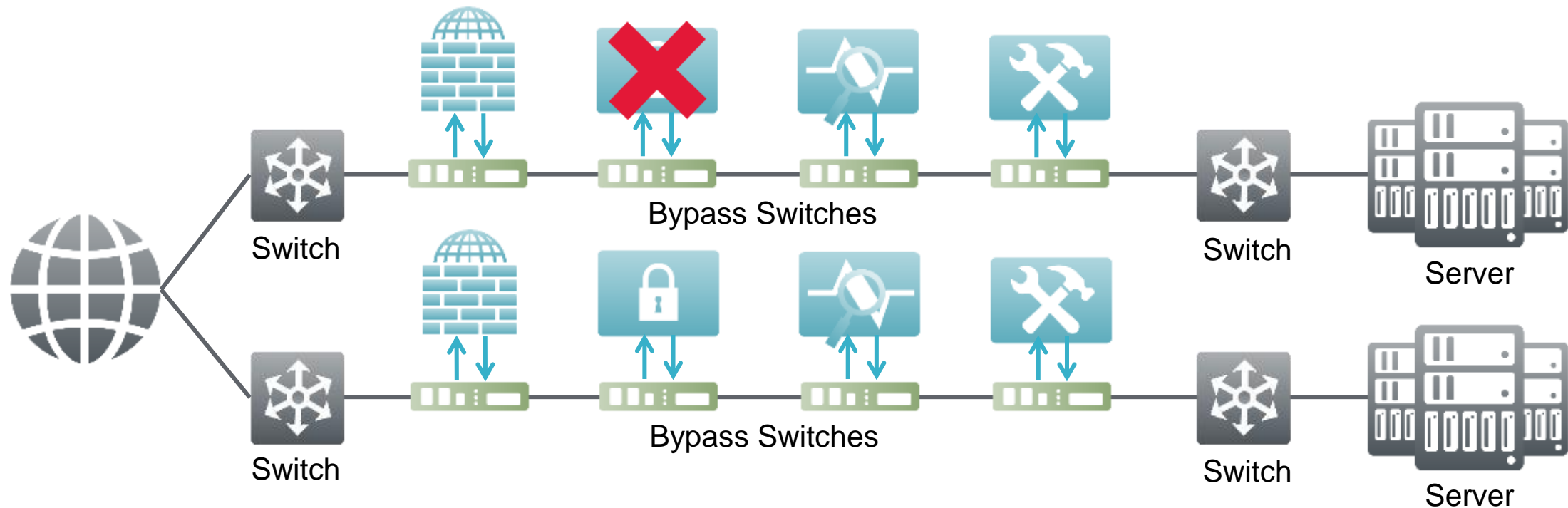
- Increased risk of downtime
- Upgrade disruption
- Inefficient use of budget and limit on ROI
- Difficult to scale
- Incomplete security monitoring

INCREASED RISK OF DOWNTIME

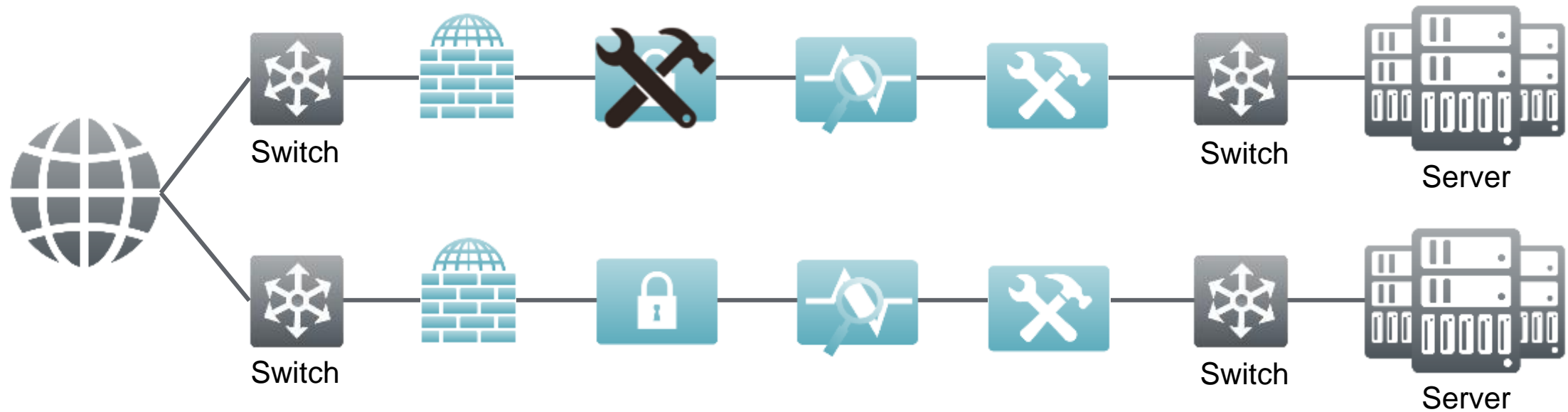


ELIMINATE DOWNTIME FROM TOOL FAILURES

→ Monitored Tool Links via Heartbeat Packets

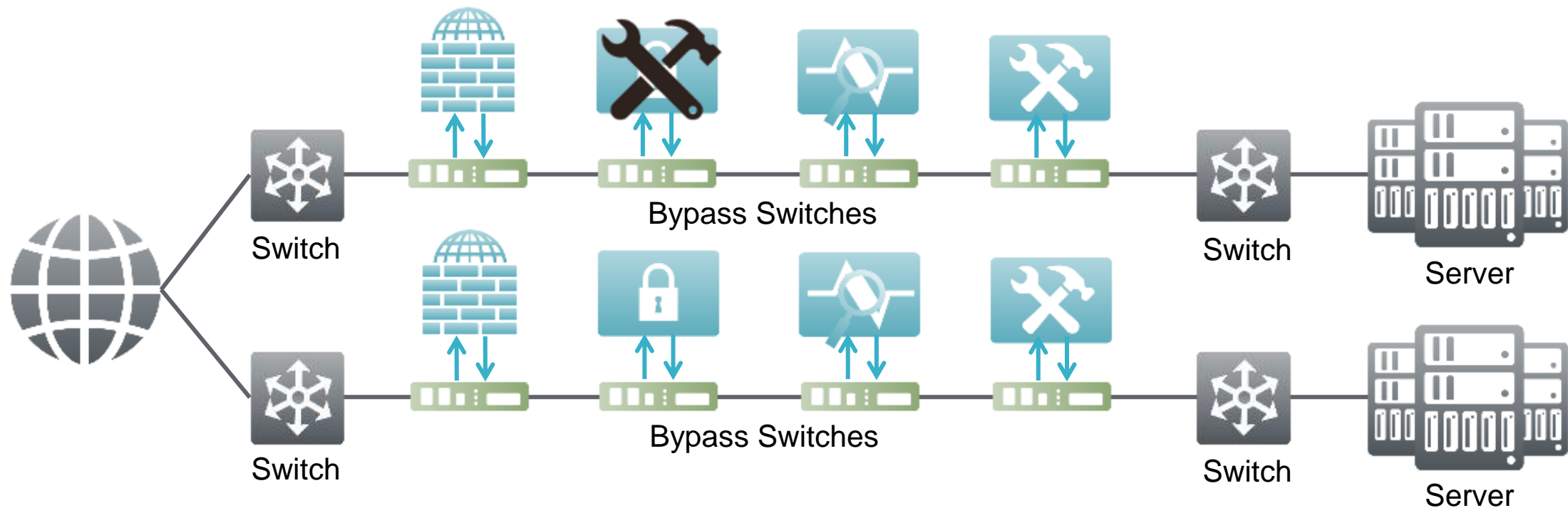


UPGRADE & MAINTENANCE DISRUPTIONS

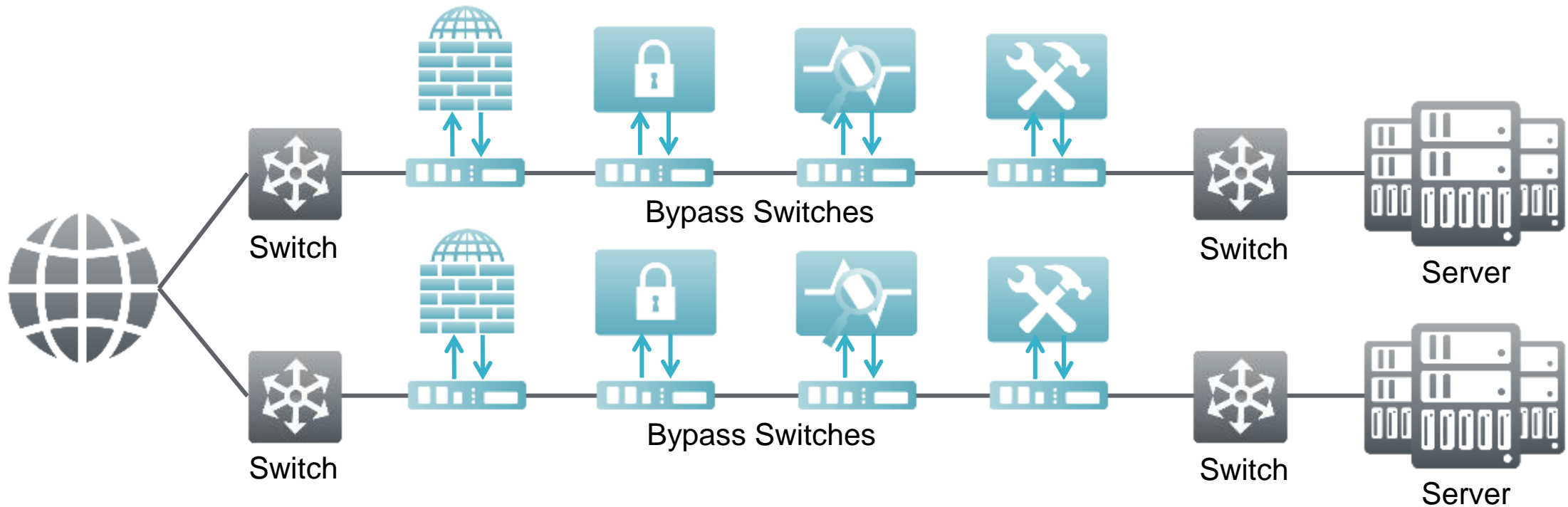


ELIMINATE UPGRADE / MAINTENANCE DISRUPTION

→ Monitored Tool Links via Heartbeat Packets



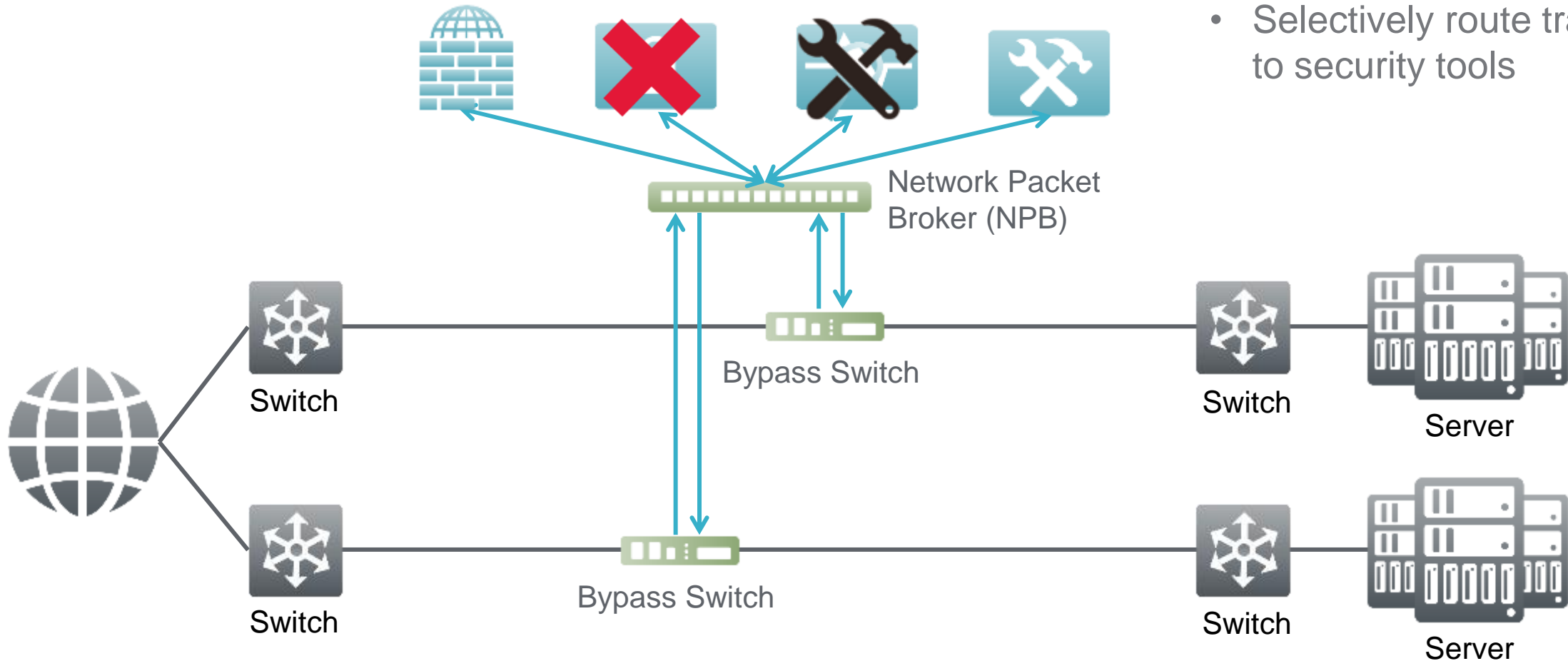
INEFFICIENT CAPACITY UTILIZATION



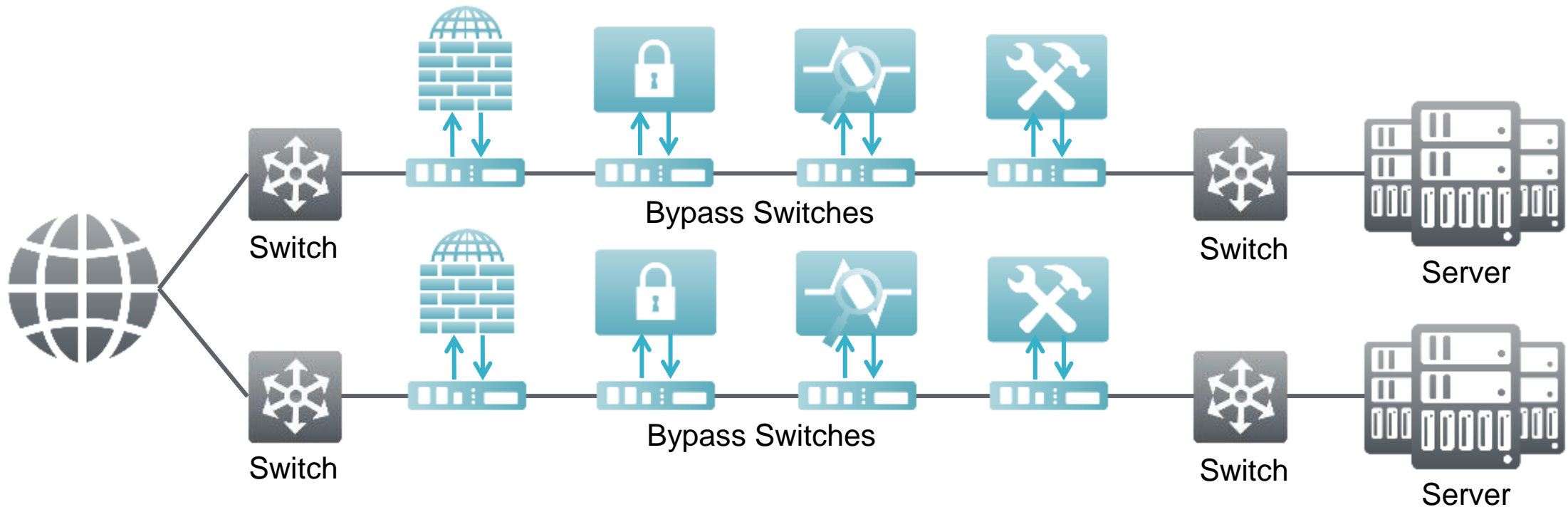
MAXIMIZE CAPACITY USAGE

→ Monitored Tool Links via Heartbeat Packets

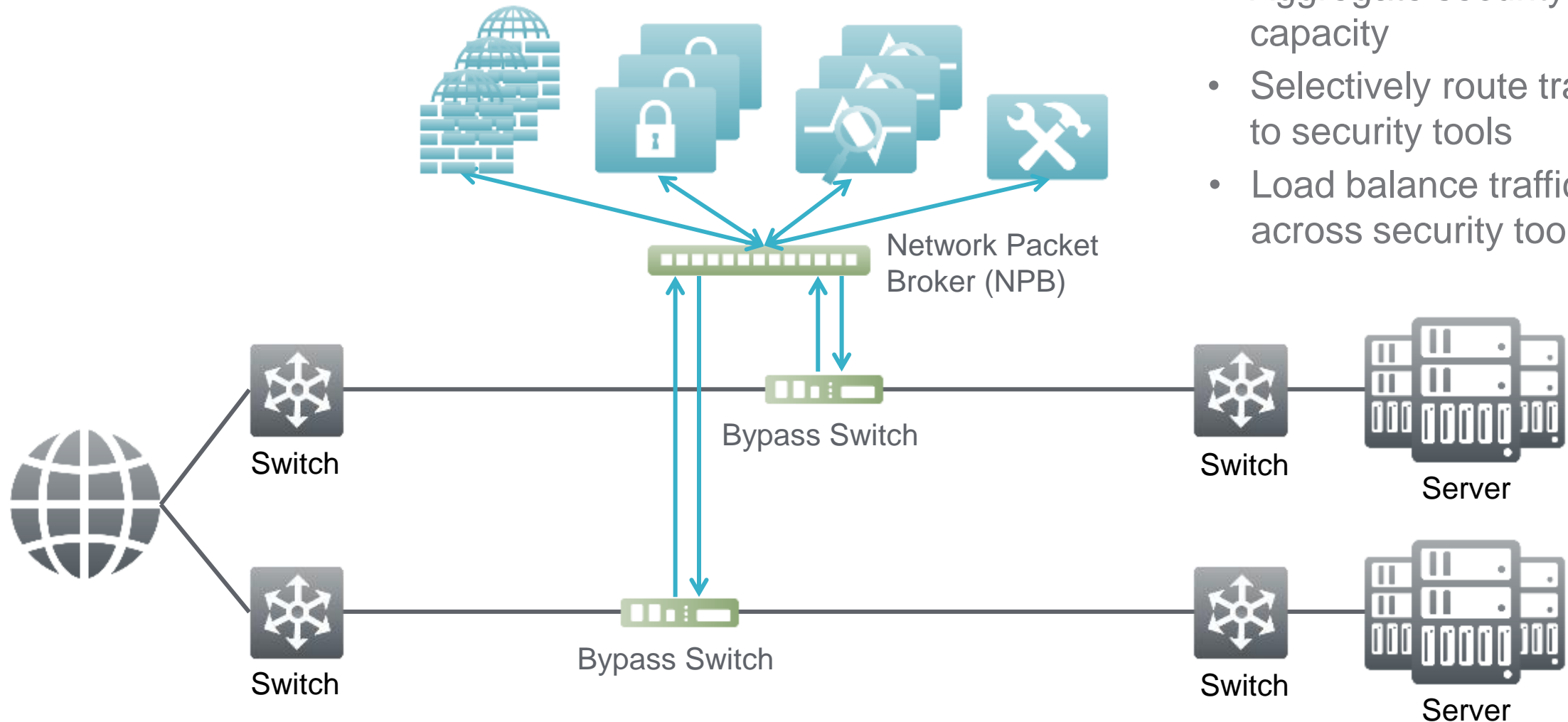
- Aggregate security tool capacity
- Selectively route traffic to security tools



DIFFICULT TO SCALE CAPACITY

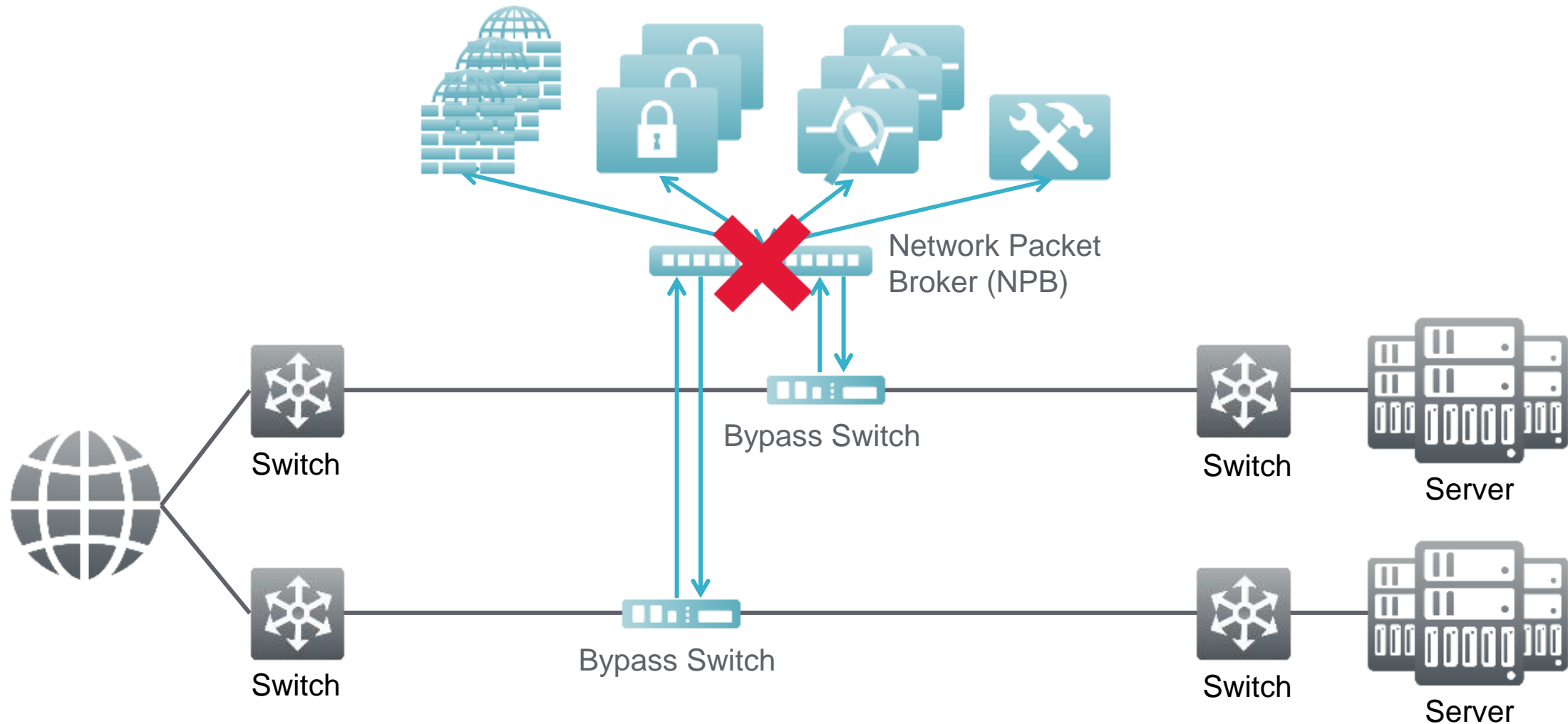


SIMPLE CAPACITY SCALABILITY

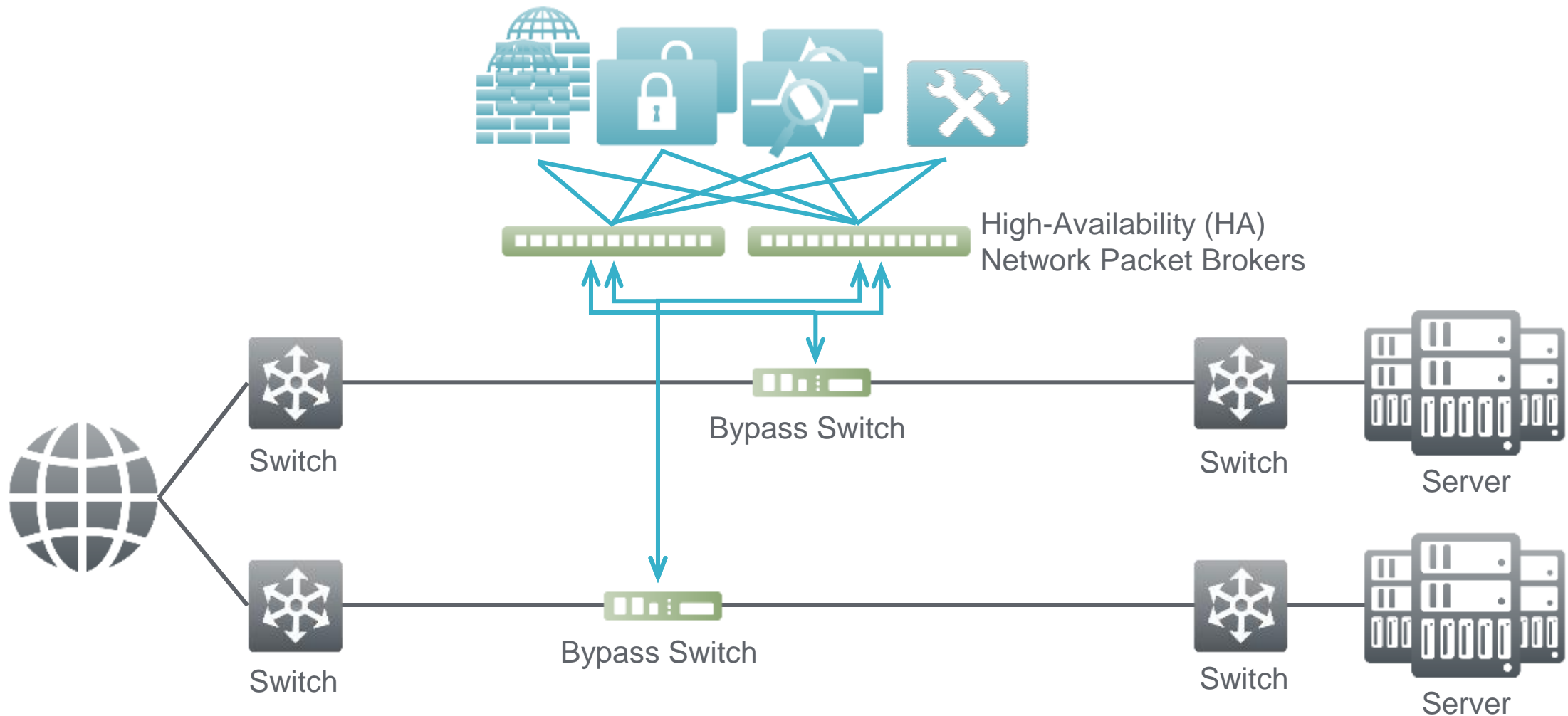


- Aggregate security tool capacity
- Selectively route traffic to security tools
- Load balance traffic across security tools

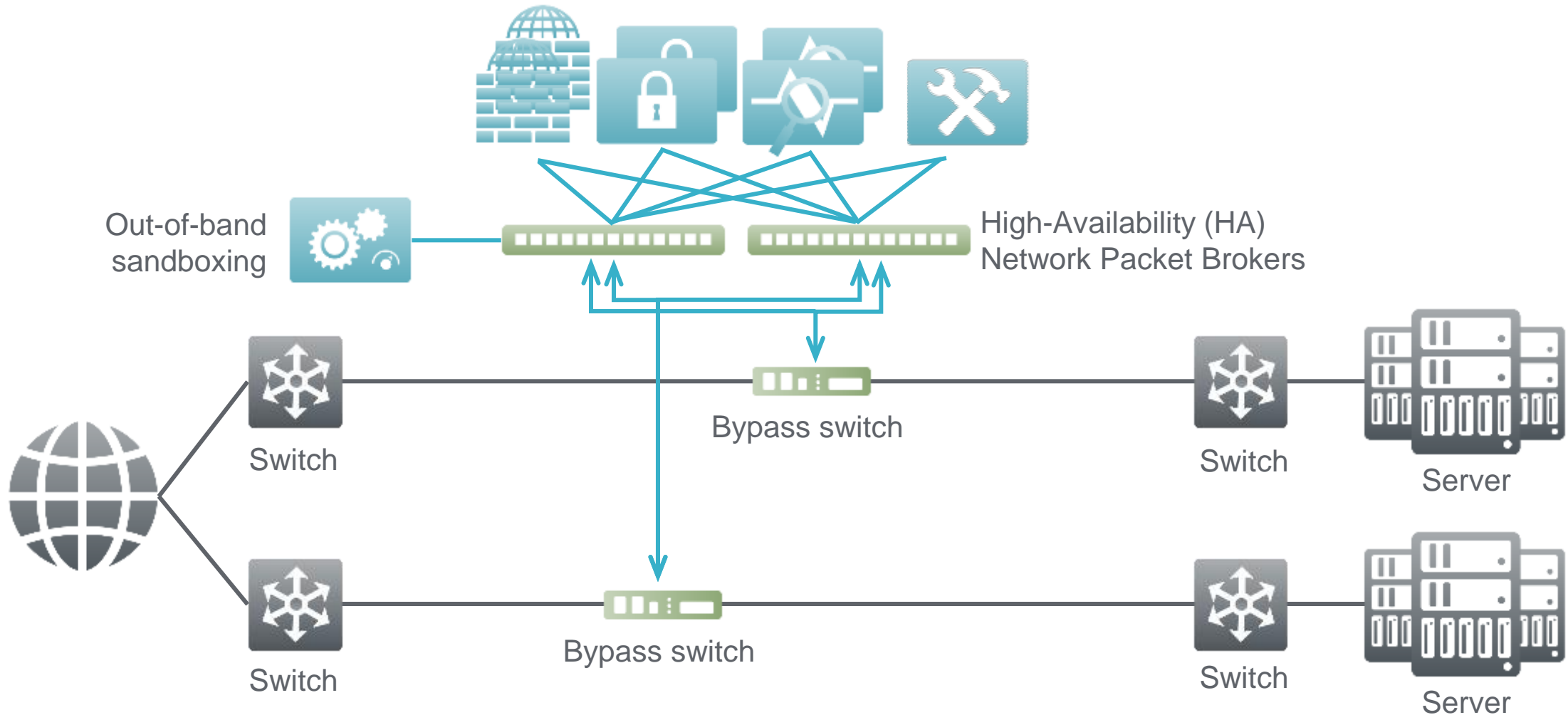
SINGLE POINT OF FAILURE



HIGH AVAILABILITY IXIA SECURITY FABRIC™



CONNECT OUT-OF-BAND SECURITY TOOLS



SUMMARY

Benefits of Deploying Ixia Security Fabric

Reduce Network Downtime

- Failsafe inline security deployments
- HA configuration with no single points of failure

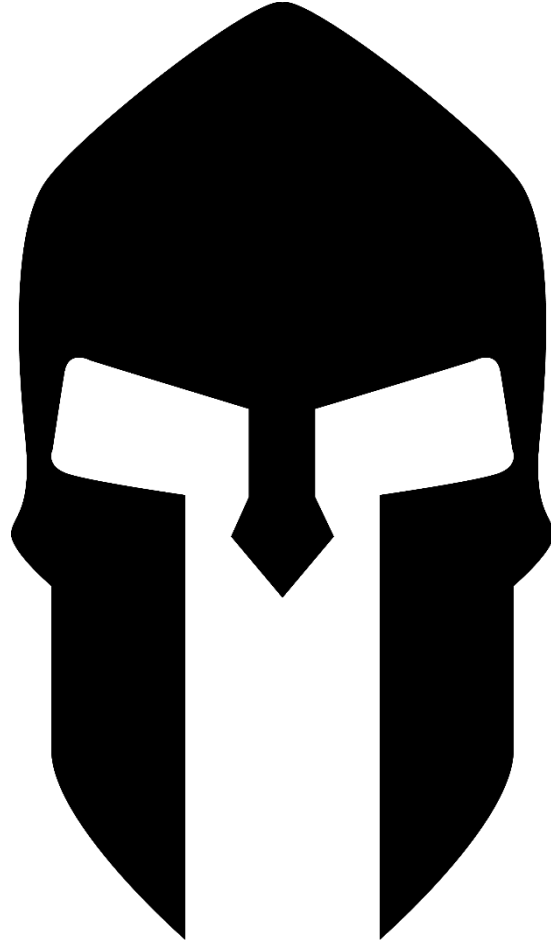
Increase Tool Efficiency

- Intelligent routing of traffic based on content
- Load balancing reduces congestion and extends tool life

Improve Inspection and Security Monitoring

- Increase monitored network segments
- Improve security resilience with HA configuration





Introducing ThreatARMOR from Ixia

ATTACK SURFACE:

THE SUM

...of every access avenue

...an attacker could use

...to enter your

network

...or

take data out.

YOUR CURRENT ATTACK SURFACE IS HUGE

Any connection to/from anywhere.

THE INTERNET



TWO TYPES OF TRAFFIC HIT EVERY NETWORK

WORTH ANALYZING:

Traffic of Possible Interest

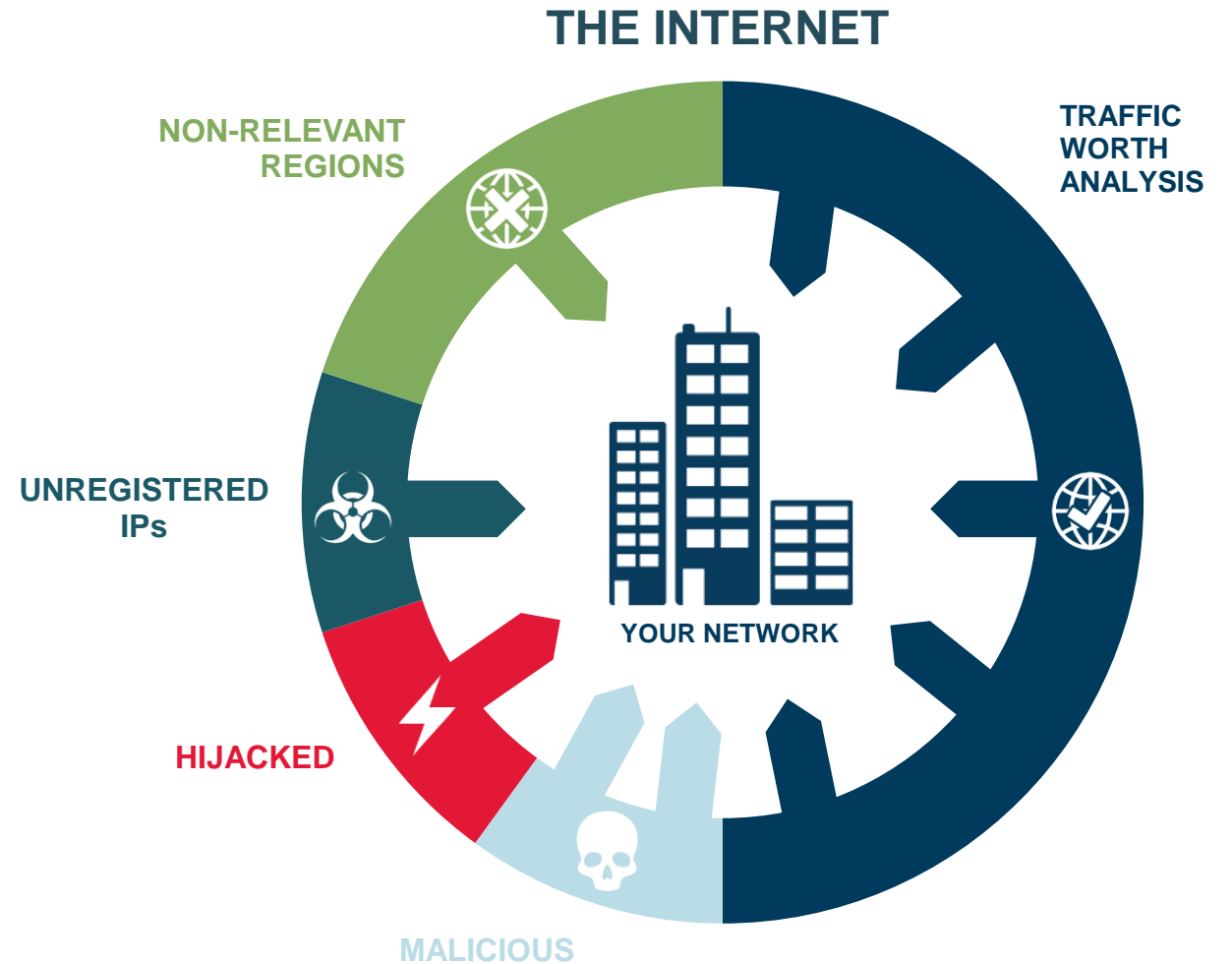
NOT WORTH ANALYZING:

KNOWN MALICIOUS

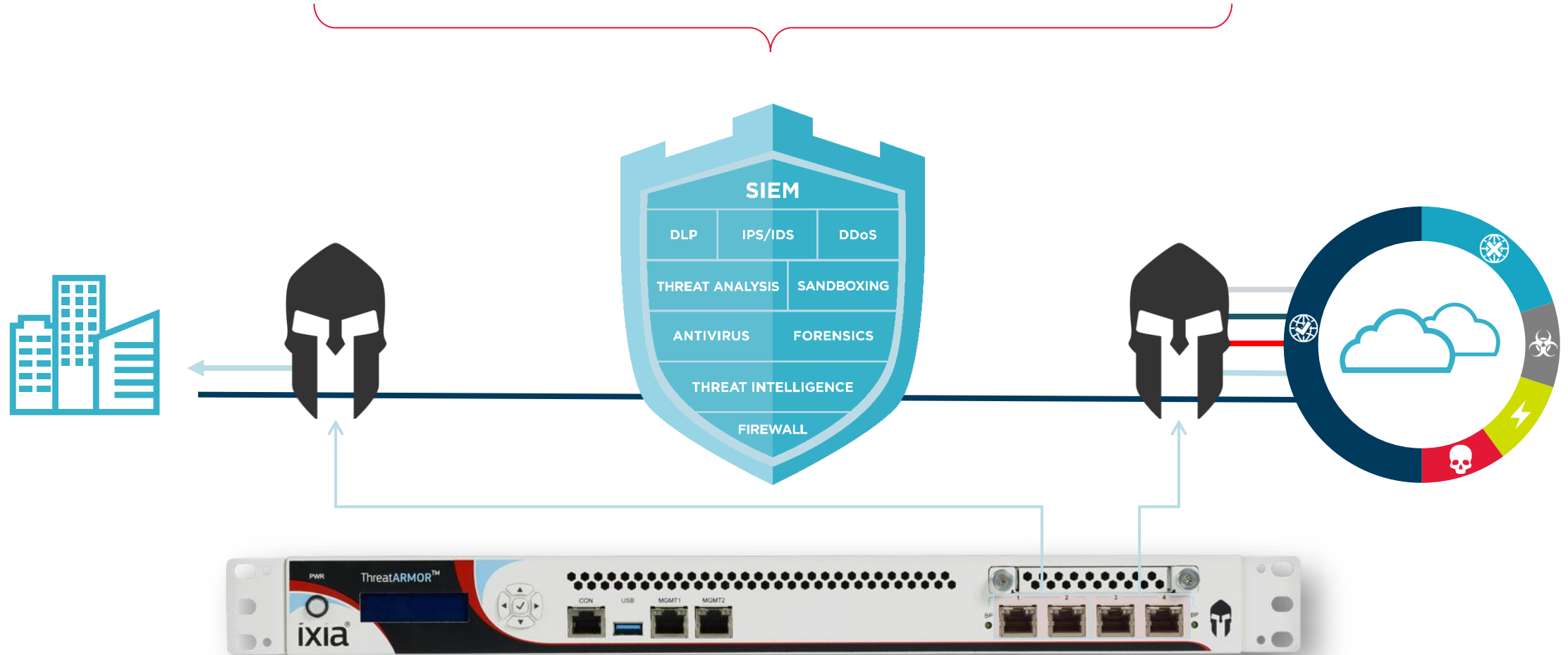
HIJACKED

UNREGISTERED IPs

UNWANTED REGIONS



ThreatARMOR is the new **security performance tool**.
Blocks known-bad IPs and eliminates untrusted countries.
Reduces alert fatigue and false positives.



Next-gen firewalls are really good at DPI, content inspection, and threat detection, but they're really bad at large-scale IP address blocking.

Why would you want to block a lot of IPs?

18% of DDoS attacks come from China

Russia, Ukraine, Pakistan, China, and Turkey are in the top 10 Botnet C&C countries

China, Brazil, Russia and India together account for 26% of web application attacks

THE PROBLEM WITH MASSIVE-SCALE BLOCKING

COUNTRY	IP RANGES
Russia	5,632
China	2,659
Pakistan	231
Turkey	644
Ukraine	2,528

CATEGORY	# OF IP ADDRESSES
Malicious Sites	> 1,000,000
Hijacked IP's	> 16,000,000
BOGONs	> 800,000,000

MOST NGFWs RUN OUT OF CAPACITY AT AROUND 10,000 RULES.

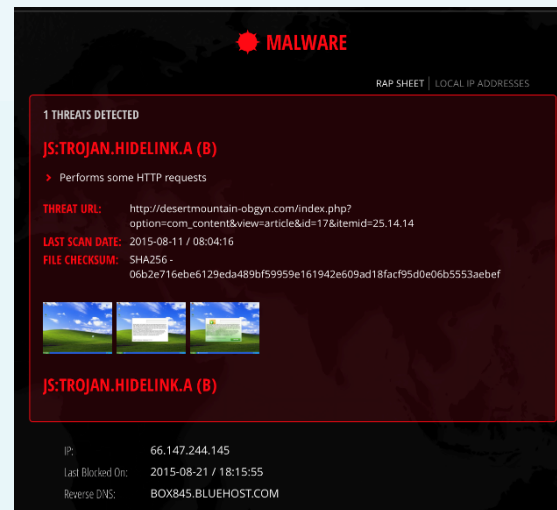
IXIA ATI Research Center

Professional-grade Threat Intelligence
used by industry leaders



ThreatARMOR Rap Sheets

Clear proof for every
blocked site.



ThreatARMOR Appliance

Set, Select and Forget.
Auto-updates every 5 min.
Maximum reliability.



LIVE RESULTS DASHBOARD

🕒 LAST WEEK ▾

0.05% THREAT ARMOR EFFICIENCY
100% FIREWALL EFFICIENCY

60.8^K
BLOCKED CONNECTIONS

132.5^M
TOTAL CONNECTIONS

1.1^{GB}
BLOCKED TRAFFIC

31.9^{TB}
Full Screen

746.15 M BITS/SEC
352 CONNECTIONS/SEC
9.88 K ACTIVE CONNECTIONS
<1% LINK UTILIZATION



TOP BLOCKED COUNTRIES

1. HONG KONG
2. UNITED STATES
3. CHINA
4. NETHERLANDS
5. INDONESIA
6. AUSTRALIA
7. GERMANY
8. UKRAINE



LAST BLOCKED IP ADDRESSES

184.168.230.1

🇺🇸 UNITED STATES

BLOCKED CONNECTIONS

35

REASON

🦠 MALWARE

2015-12-16 10:15:50

193.104.41.54

🇲🇵 REPUBLIC OF M...

BLOCKED CONNECTIONS

62

REASON

🦠 EXPLOIT

2015-12-16 10:06:25

97.74.158.1

🇺🇸 UNITED STATES

BLOCKED CONNECTIONS

3

REASON

🦠 MALWARE

2015-12-16 09:50:50

43.229.53.55

🇭🇰 HONG KONG

BLOCKED CONNECTIONS

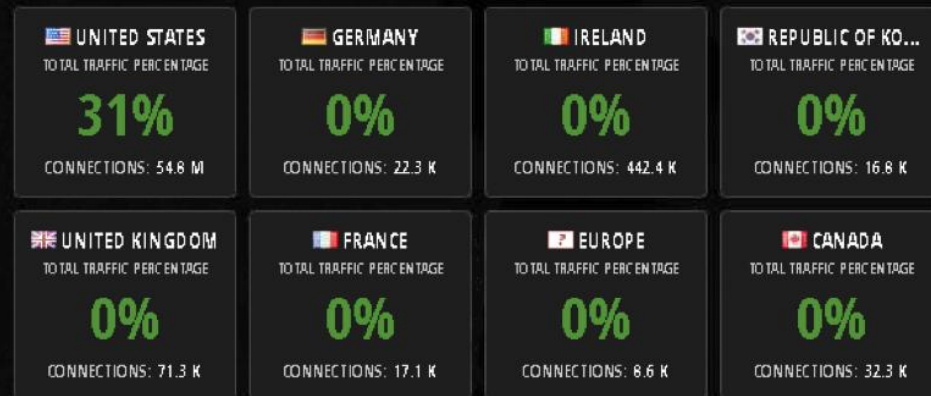
54.1 K

REASON

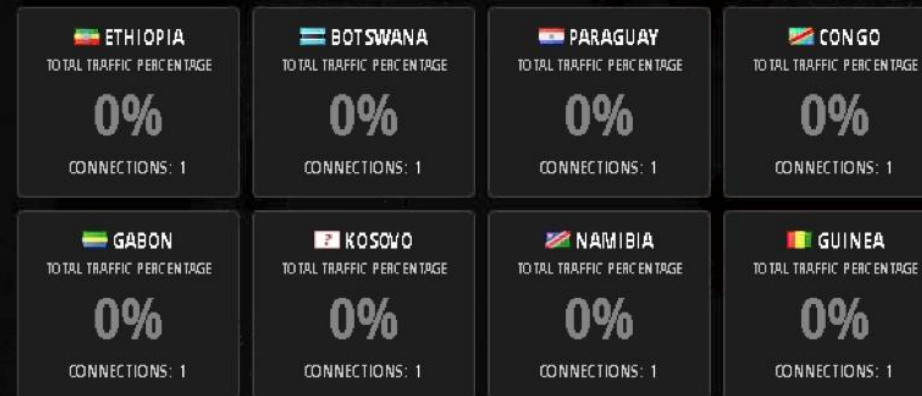
⚡ HIJACKED

2015-12-16 09:49:29

TOP ALLOWED COUNTRIES



BOTTOM ALLOWED COUNTRIES



LIVE RESULTS: RAPSHEET

ixia

ThreatARMOR

[scooper@causewaycap.com]



















































5  


DASHBOARD



DASHBOARD \ BLOCKED IP ADDRESSES

🕒 LAST WEEK ▾

IP Address	Country	Reason	Last Blocked On
115.85.192.40	 China		2015-12-11 20:45:02
185.112.102.222	 Russia		2015-12-11 20:02:55
119.82.226.9	 Indonesia		2015-12-11 17:29:23
42.54.161.112	 China		2015-12-11 17:29:21
42.55.96.254	 China		2015-12-11 17:25:48
222.186.52.95	 China		2015-12-11 15:38:02
98.138.19.143	 United States		2015-12-11 14:51:36
173.201.233.1	 United States		2015-12-11 14:46:56
81.169.145.163	 Germany		2015-12-11 14:44:31
104.200.78.34	 Netherlands		2015-12-11 14:24:55
45.10.0.111	 Unassigned-IP		2015-12-11 12:08:23
97.74.47.1	 United States		2015-12-11 11:54:53
184.168.204.1	 United States		2015-12-11 10:46:27
81.169.145.66	 Germany		2015-12-11 10:18:24
184.106.55.101	 United States		2015-12-11 10:17:16
50.63.223.1	 United States		2015-12-11 10:14:38
50.62.231.1	 United States		2015-12-11 09:59:18
42.54.7.8	 China		2015-12-11 09:58:37
50.63.88.1	 United States		2015-12-11 09:45:50
97.74.215.189	 United States		2015-12-11 09:05:25
68.178.254.16	 United States		2015-12-11 08:59:02
192.145.239.17	 United States		2015-12-11 08:18:01
98.129.229.75	 United States		2015-12-11 07:26:36
208.67.1.25	 United States		2015-12-11 06:33:44
37.187.240.219	 France		2015-12-11 06:31:17
109.169.48.102	United Kingdom		2015-12-11 04:44:50

Showing last 100 blocked IP addresses  REFRESH

LOAD MORE RESULTS

IP:45.10.0.111

 RULE: BLOCK UNASSIGNED IP ADDRESSES

RAP SHEET | LOCAL IP ADDRESSES

Unassigned IP addresses are characterized by ThreatARMOR to be invalid on the Internet: IP addresses which have not been properly allocated by IANA or an RIR which appear on ThreatARMOR's Internet-facing interface.

Reverse DNS: 45.10.0.111

Last Blocked On: 2015-12-11 12:08:23

384_B

BLOCKED TRAFFIC

6

BLOCKED PACKETS

1

BLOCKED CONNECTIONS

264.4_{KB}

EST. BANDWIDTH SAVED

LIVE RESULTS: RAPSHEET 2

🔍 🌐 LAST WEEK ▾

IP Address	Country	Reason	Last Blocked On
97.74.144.189	🇺🇸 United States	☀️	2015-12-14 13:45:32
184.168.137.1	🇺🇸 United States	☀️	2015-12-14 13:04:55
50.63.77.1	🇺🇸 United States	☀️	2015-12-14 13:02:19
43.229.53.89	🇭🇰 Hong Kong	⚡	2015-12-14 12:12:16
98.129.229.174	🇺🇸 United States	☀️	2015-12-14 11:54:15
173.201.242.1	🇺🇸 United States	☀️	2015-12-14 10:48:44
218.25.208.92	🇨🇳 China	🦠	2015-12-14 10:23:59
184.168.203.1	🇺🇸 United States	☀️	2015-12-14 09:50:05
46.252.201.1	🇳🇱 Netherlands	☀️	2015-12-14 08:47:32
185.68.16.23	🇺🇦 Ukraine	☀️	2015-12-14 08:45:52
173.201.96.128	🇺🇸 United States	☀️	2015-12-14 08:30:15
50.63.38.1	🇺🇸 United States	☀️	2015-12-14 07:13:28
1.93.51.221	🇨🇳 China	🦠	2015-12-14 06:55:26
222.186.34.238	🇨🇳 China	🦠	2015-12-14 01:25:57
115.231.219.252	🇨🇳 China	🦠	2015-12-13 21:17:34
68.168.209.242	🇺🇸 United States	☀️	2015-12-13 19:38:28
42.52.49.2	🇨🇳 China	⚡	2015-12-13 19:10:19
42.52.120.72	🇨🇳 China	⚡	2015-12-13 18:51:31
42.52.236.224	🇨🇳 China	⚡	2015-12-13 18:43:27
42.53.79.10	🇨🇳 China	⚡	2015-12-13 18:26:10
42.52.120.57	🇨🇳 China	⚡	2015-12-13 18:24:57
42.53.37.152	🇨🇳 China	⚡	2015-12-13 18:19:39
103.1.175.1	🇸🇬 Singapore	☀️	2015-12-13 11:21:18
222.186.21.181	🇨🇳 China	🦠	2015-12-13 05:26:46
42.52.26.189	🇨🇳 China	⚡	2015-12-12 18:20:33
50.56.185.103	🇺🇸 United States	🦠	2015-12-12 18:05:49

Showing last 100 blocked IP addresses 🔄 REFRESH

[LOAD MORE RESULTS](#)

RAP SHEET | LOCAL IP ADDRESSES

LAST SCAN DATE 2015-11-30 23:19:34

FILE CHECKSUM SHA256 - a7220d02baca772cdba7fe63f8a734662a0ec37d83f66acb98031f3b2d0ede69

JS/AGENT.NNS TROJAN

THREAT URL http://suzirjaukr.com/en/component/users/

LAST SCAN DATE 2015-12-16 03:55:47

FILE CHECKSUM SHA256 - c4fb46c5005d61a936dcc2e3b352baa0ab476d7f199abe9d658e42fc2381eb77

PAGE TITLE Алерго Хортиці



JS/AGENT.NNS TROJAN

THREAT URL http://anna.suzirjaukr.com/ru/gallery/2011

LAST SCAN DATE 2015-12-15 02:24:27

FILE CHECKSUM SHA256 -

Reverse DNS: 185.68.16.23

Last Blocked On: 2015-12-14 08:45:52

360.3 KB

BLOCKED TRAFFIC

312

BLOCKED PACKETS

9

BLOCKED CONNECTIONS

2.4 MB

EST. BANDWIDTH SAVED

The logo for ixia is displayed on a 3D cube. The cube is light blue on the left side and a darker blue on the right side. The text 'ixia' is white, with a red dot above the 'i' and a blue dot above the 'a'.

ixia

THANK YOU