Putting
IPv6
to work

North American IPv6 Summit

Grand Hyatt, Denver, Colorado
September 23-25, 2014

Rocky Mountain IPv6 Task Force
RMv6TF

IPv6 and DDoS Protection: Securing Carrier Grade NAT Infrastructure

Glen Turner
Consulting Systems Engineer
IPv6 Migration Technologies
A10 Networks
gturner@a10networks.com

DDoS Attack Trends and Effects

Q3 2010
PayPal
Discloses cost of attack £3.5M (~$5.8 million)

Q4 2012
Bank of the West
$900k stolen, DDoS as a distraction

Q1 2013
al Qassam Cyber Fighters
10-40 Gbps attacks target 9 major banks

Q1 2013
Credit Union Regulators
Recommend DDoS protection to all members

Q1 2014
CloudFlare
400 Gbps NTP amplification attack

Q4 2013
60 Gbps attacks regularly seen,100 Gbps not uncommon

Q4 2013
26% YoY attack increase (17% L7, 28% L3-4)

Q4 2013
PPS reaches 35 million

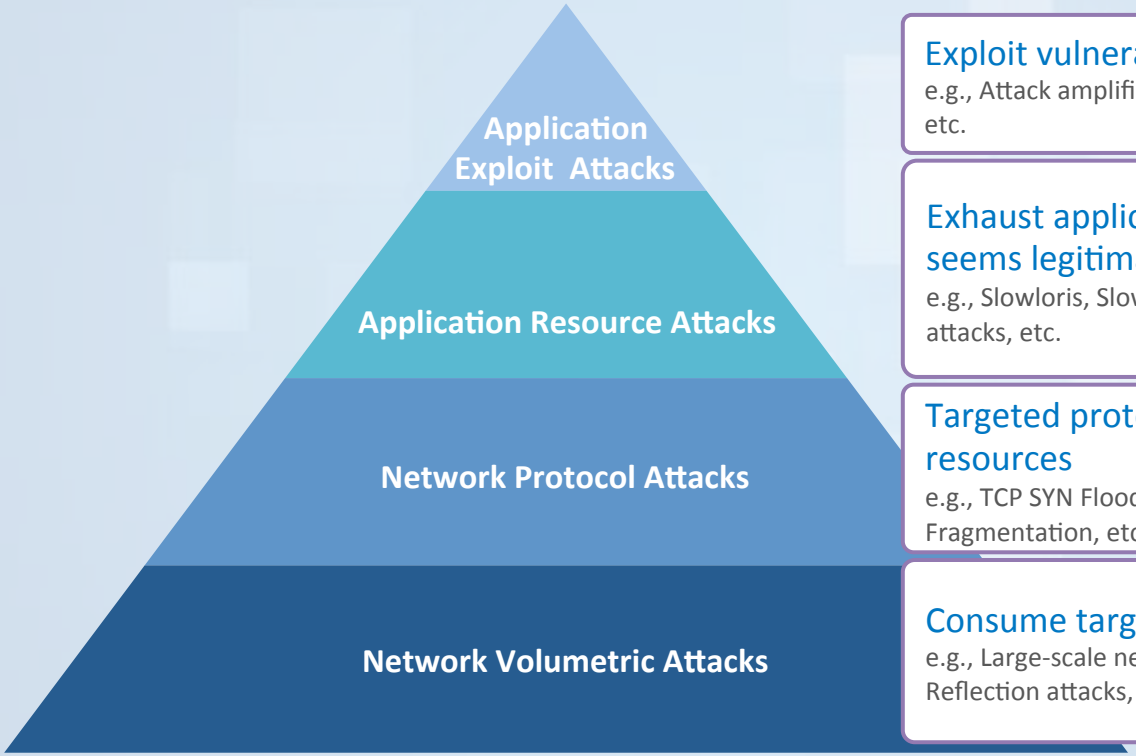
Q4 2013
6.8 million mobile devices are potential attackers

"High-bandwidth DDoS attacks are becoming the new norm and will continue wreaking havoc on unprepared enterprises."

Gartner Press Release, "Gartner Says 25 Percent of Distributed Denial of Services Attacks in 2013 Will Be Application-Based," February 21, 2013. http://www.gartner.com/newsroom/id/2344217

Rocky Mountain IPv6 Task Force
RMv6TF

DDoS Threat Pyramid



Exploit vulnerabilities in the application
e.g., Attack amplification (for NTP/DNS, etc.), buffer overflows, etc.

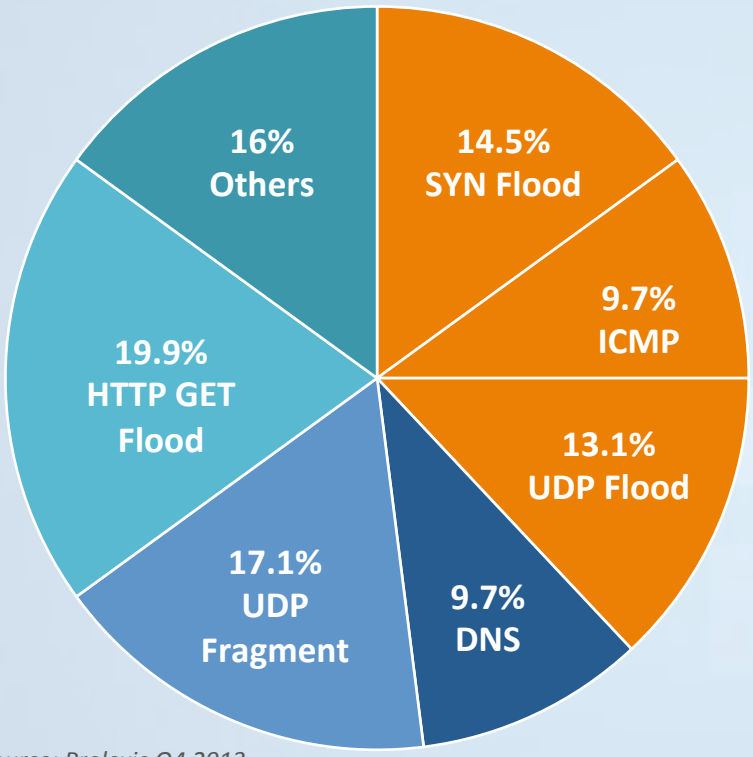
Exhaust application resources using traffic that seems legitimate
e.g., Slowloris, Slow READ, R.U.D.Y, Slow POST, HTTP GET attacks, etc.

Targeted protocol attacks to exhaust specific resources
e.g., TCP SYN Flood, Ping of Death, LAND attack, Fragmentation, etc.

Consume targets' bandwidth
e.g., Large-scale network protocol attacks, including DNS/NTP Reflection attacks, UDP Flood, ICMP Flood, etc.

Rocky Mountain IPv6 Task Force
RMv6TF

DDoS Attack Types Observed



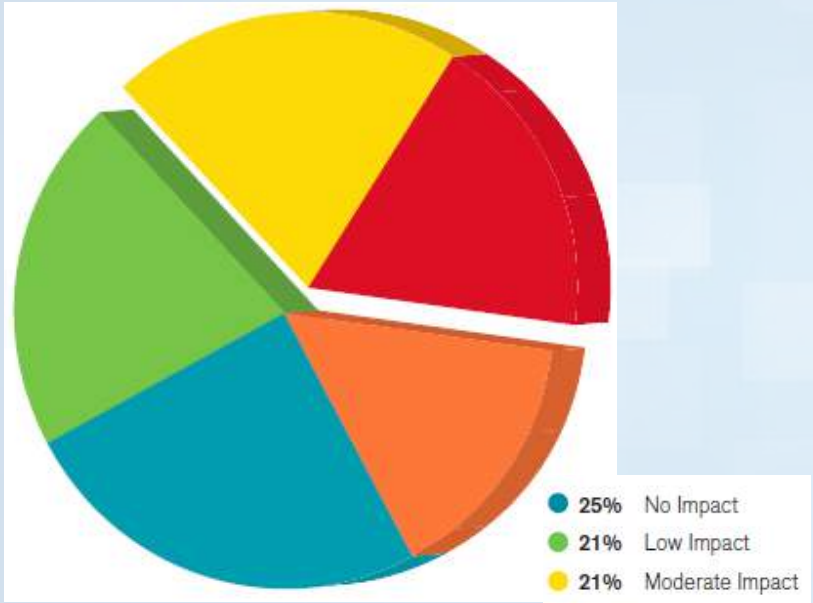
Source: Prolexic Q4 2013

- The largest attacks increase 33%
  - 300 Gbps (Q2 2013)
  - 400 Gbps (Q1 2014)
- 60 Gbps regularly seen, 100 Gbps not uncommon
- Average attack packets-per-second
  - 35 million PPS

Rocky Mountain IPv6 Task Force
RMv6TF

CGN Device Targeted DDoS Attacks

Impact of Attacks Against NAT Infrastructure



Source: Arbor Infrastructure Security Report

CGN Attack Vectors

- Volumetric
- State Exhaust
- 81% of total DDoS attacks
- Vulnerable to both internal and external attacks
  - Internal attacks more difficult to mitigate

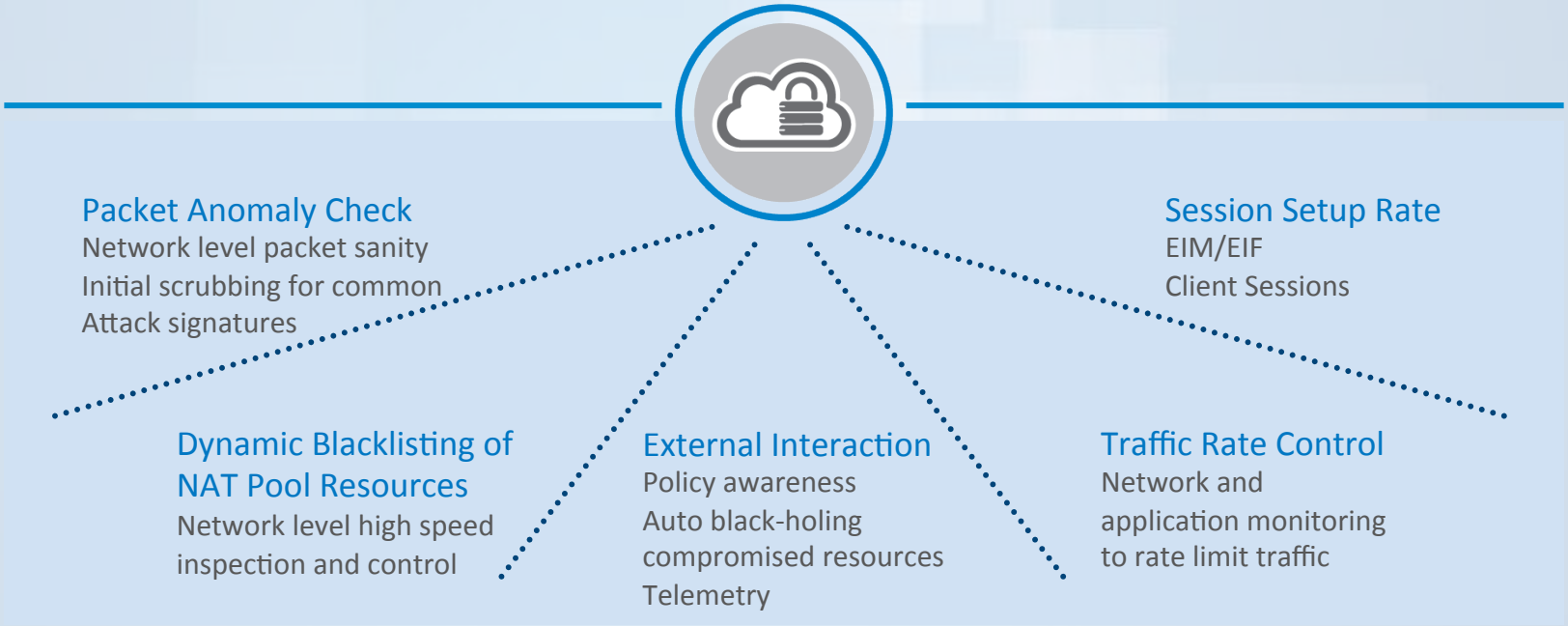
CGN Vulnerabilities

- UDP/TCP State Exhaust
- Volumetric Attacks against NAT Pool Resources
- Excessive Client Port Allocation Requests
- Client session setup rate
- EIM/EIF session creation
- EIM/EIF session setup rate
- Indirectly affects logging infrastructure

Rocky Mountain IPv6 Task Force
RMv6TF

Mitigating CGN Device DDoS Attacks

Fundamental requirements for effective mitigation



Rocky Mountain IPv6 Task Force
RMv6TF

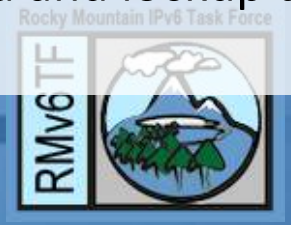
CGN Security

IP Anomaly Filter

- Detects and drops packets containing common attack signatures for all incoming ports
- Ensures properly formatted packets and adherence to standards and state machines
- Protects against attacks based upon known packet signatures
- Disrupts network reconnaissance attempts in which attackers may use protocol vulnerabilities to gain target information such as operating system type and version

ICMP Rate Limiting

- Mitigates ICMP volumetric attacks
- Supports both IPv4 and IPv6
- Provide watermarks for ICMP drop per second and lockup time
- Lockup events logged

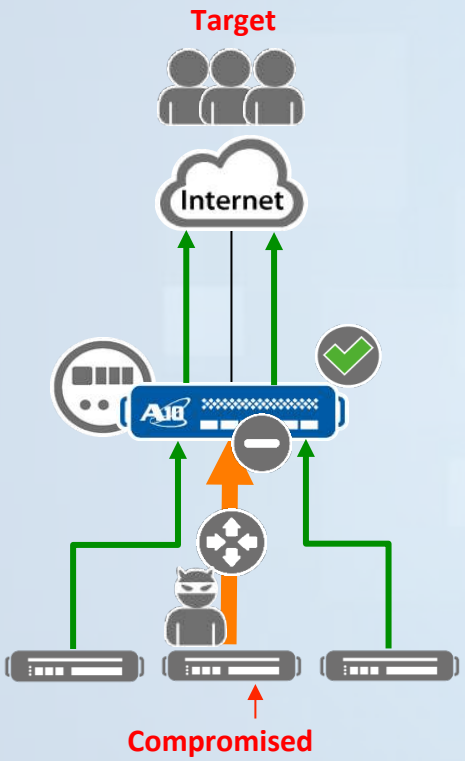


CGN Security

IP Anomaly Filter

Detects and drops packets containing common attack signatures for all incoming ports		
LAND Attack	Bad IP Checksum	TCP Fragmented Header
Empty Fragment	ICMP Ping of Death	TCP Bad Checksum
Micro Fragment	TCP Bad Urgent Offset	UDP Short Header
IPv4_Options	TCP Short Header	UDP Bad Length
IP Fragment	TCP Bad IP Length	UDP Kerberos Frag
Bad IP Header Length	TCP Null Flags	UDP Port Loopback
Bad IP Flags	TCP Null Scan	UDP Bad Checksum
Bad IP TTL	TCP Syn & Fin	Runt IP Header
No IP Payload	TCP XMAS Flags	Runt TCP/UDP Header
Oversize IP Payload	TCP XMAS Scan	IP Tunnel Mismatch
Bad IP Payload Length	TCP Syn Fragment	
Bad IP Fragment		

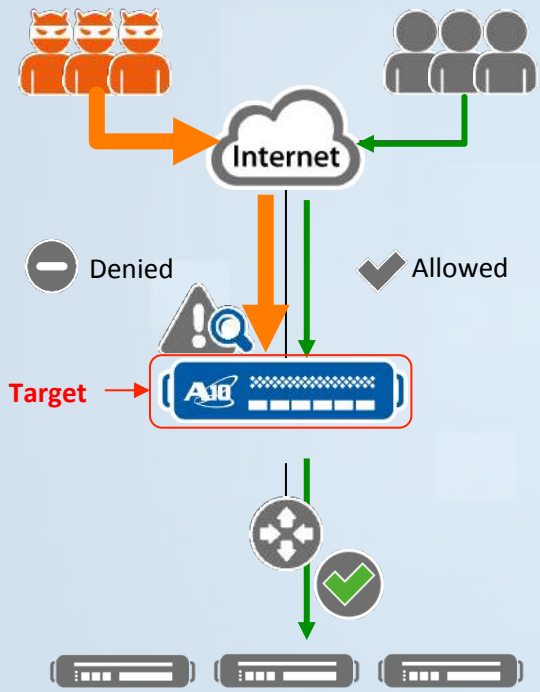
CGN Device Targeted DDoS Attacks



- Enforcement of connections setup rate for mitigation of flood based attacks (e.g., TCP SYN, UDP, and ICMP flooding)
- Rate limits per source IP address
  - Limits connection rate from both inside and outside originating flows
    - Applicable for EIF Sessions
    - Maximum absolute inside/outside connections capped by session-quota
    - Maximum absolute inside connections capped by user quota
- If CPS limit is exceeded, sessions are no longer created for the source IP address
  - CPS limit will inhibit new session creation even if user/session quotas are not exceeded
- Policy aware traffic policing
- Support for hair-pinned sessions

Rocky Mountain IPv6 Task Force
RMv6TF

CGN Security-NAT Pool Resource Protection



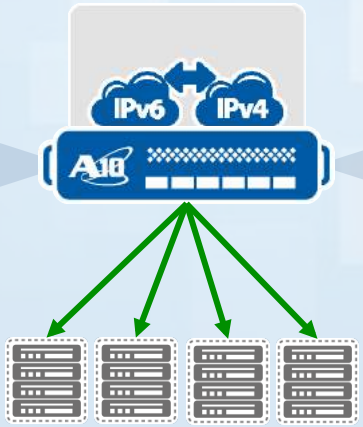
- Provides device protection from volumetric attacks targeting NAT pool resources by dropping packets early in data path prior to reaching L4-L7 processes
- Operator defined threshold can be set for IP, TCP, UDP
- If thresholds are violated, 2-tuple entry for NAT IP/ Port written into software/hardware tables
- Packets that match table entries exceeding thresholds are dropped
- Entries age out within 10secs after falling below threshold

Rocky Mountain IPv6 Task Force
RMv6TF

CGN Security-Telemetry and Analytics

Global Statistics	
TCP Received	73567367
TCP Out of Order Timer Expired	367367
TCP Out of Order	373
TCP Retransmitted FIN	54737
TCP Retransmitted PSH	4645
TCP Retransmitted RST	3456345
TCP Retransmission	2356
TCP RST	34563
TCP SYN Received	534563
TCP SYNs per second	345634563
TCP established	345634
HTTP too many headers	34563456
HTTP Header name too long	66565
HTTP 1.0	54564
HTTP 1.1	34735
HTTP Get	367567
HTTP Head	43676
HTTP Post	467567
HTTP Trace	675676
HTTP Options	345645
HTTP Connection	45643
HTTP Delete	34565
HTTP Unknown	456454
HTTP request line too long	4574
HTTP request length too long	47454
HTTP partial header	4767
HTTP Slow Post	45645
HTTP Bad Chunk	47457
HTTP Chunk < 512	675675
HTTP Chunk < 1k	47457
HTTP Chunk < 2k	457457
HTTP Chunk < 4k	45745
HTTP chunk > 4k	67567
HTTP response chunk	457457
HTTP parse request failure	454
HTTP request	67457
HTTP Client RST	47567
HTTP Request retransmit	6756
HTTP request out of order	457454
HTTP invalid header	235
HTTP payload too small	4574
HTTP destination request rate exceeded	4574
HTTP source request rate exceeded	457474
HTTP packets processed	457454
HTTP out of order queue exceeded	457454

- sFlow using multiple extensions
- IPFix
- Common Event Format Logging
- On box packet captures



xFlow Collection Infrastructure

Per IP Statistics	131.107.4.2	131.107.2.4	131.17.17.8
TCP packets	343452345	23452345	526256
UDP packets	262346	646	457
ICMP packets	5	5775	4574
IPv6 packets	775	6456456	34665
IPSec packets	575	3564574574	34644
IGMP packets	575	477754	5575
"Other IP Protocols"	678	4776	55453
TCP SYN	678	7676	343
TCP SYN/Ack	9777	25	1222
TCP Fin	679	35645	232
TCP RST	69	4574	780
TCP URG	568	45353	568586
Total Packets	5666	45745	45345
concurrent HTTP connections	56856	6865	566
New HTTP connections	566776	675	56856
Avg between request and response	56765	5866	5665
total ingress/egress bandwidth	5676	568568	56865
Number of occurrence of each method	5676	3434	34643
blocked packets due to countermeasures	56756	677	34646
US conns	346345	343	343
FR conns	345	53454	34545
CN conns	3453	345	223

Rocky Mountain IPv6 Task Force
RMv6TF

CGN Security-Implementation Guidelines

- Access Control Lists for device-wide permissions and OAM access
- Configure the CGN device to drop all subscriber packets from source IP addresses not explicitly defined. Add 0.0.0.0/0 to the client policy list and explicitly drop this traffic
- Disabling inbound-refresh can provide protection against malicious applications and DDoS attacks
- Implement a TCP SYN defense method
- Optimize subscriber port allocations (aka user-quota)
- Disable ICMP Ping response for NAT pool addresses
- Disable unused ALG and secure ALG in use

Rocky Mountain IPv6 Task Force
RMv6TF

CGN Security-Implementation Guidelines

- Limit EIM/EIF attack vectors
  - Operators should set session quotas to limit fullcone NAT sessions
  - Set STUN timers in accordance with network application requirements
  - Use connection rate limiting to limit full-cone session creation, configure per-protocol full-cone behavior, and limit full cone sessions per port

- Expedite log correlation by explicitly configuring logging (syslog/traffic logging) to include subscriber information such as client source IP address and other user attributes provided through custom Radius attributes (e.g., MSISDN/IMSI, user name)
- DDoS attacks could exceed trigger thresholds for multiple mitigation techniques. Understand your CGN device's architecture to determine the most efficient mitigation strategy that optimizes operational behavior

Questions?

Glen Turner

gturner@a10networks.com

Thank You

Glen Turner

gturner@a10networks.com