RESILIENCE

STRENGTHENING NETWORK RESILIENCE THROUGH DDOS MITIGATION TACTICS

KNIGHT SHIFT IT
Secure. Reliable. Automated.

Hello!

Adam Ahad Aboss
CTO at Knight Shift IT Pty Ltd
Network Architect
PacNOG 32

- ahad@knightshiftit.com.au
- https://www.knightshiftit.com.au
- +61 478 509 000
- +61 2 9159 9194

KNIGHT SHIFT IT
Secure. Reliable. Automated.

INTRODUCTION

LAYING THE FOUNDATION FOR A RESILIENT AND SECURE NETWORK

- A resilient network can maintain continuity through disasters and cyber attacks
- Network outages can cost $100Ks - resilience is critical
- Proactive security prevents outages and data loss
- Threats are escalating - DDoS and ransomware attacks has been on the increase yearly
- Cloud, IoT and high-speed mobile introduce new attack surfaces
- Advanced techniques like BGP FlowSpec are essential for control

STEP 1

SECURITY CHECKLIST FOR YOUR NETWORK INTERCONNECTS

NETWORK IX CHECKLIST

- Boundaries are first line of defence against DDoS
- Analyse ingress/egress points for vulnerabilities:
  - Peering & transit links
  - CDNs & caches
  - Backhaul providers
- Implement real-time monitoring. Don’t simply trust your IX Peer.
  - sFlow, NetFlow sampling, alerting & analysis
  - Reduced counter timers ONLY if you have enough resources
- Deploy ACLs and advanced protocols:
  - Authentication requirements
  - Rate limiting & bandwidth control
- Build redundancy & failover mechanisms
- Unify with partners across ecosystems

KNIGHT SHIFT IT
Secure. Reliable. Automated.

STEP 2

SECURE YOUR LAYER 2 DOMAIN

KNIGHT SHIFT IT
Secure. Reliable. Automated.

SECURING LAYER 2

- Boundaries are first line of defence against DDoS
- Layer 2 attacks exploit broadcast traffic, VLANs, and switching
- Implement storm control, BPDU guard against exploits
- Optimize VLANs to segment security domains
- Require port security and ARP inspection
- Use 802.1X for robust device authentication

- **Case study:** Akamai switch caused nationwide outage– Australian ISP
  - BPDU flooding brought down production network
  - BPDU guard and Storm control could have prevented blast radius

SECURING LAYER 2:
KEY PRACTICES

- Harden configurations at all levels
- Authenticate connected devices – Filter Mac addresses
- Detect protocol anomalies with monitoring sensors
- Contain blast radius with controls
- Implement storm control, BPDU guard and other port security measures against exploits
- Monitor protocols, hardware state, memory and cpu utilisation to detect anomalies in advance

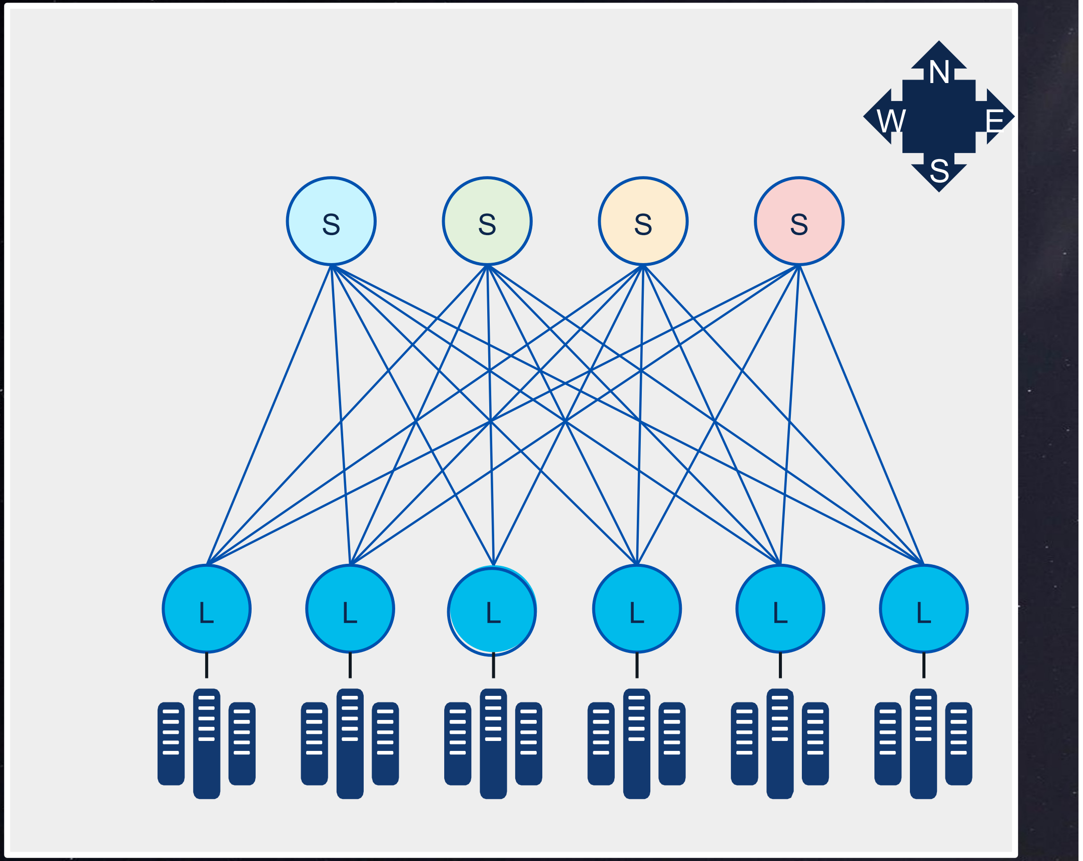
SECURING LAYER 2: SPINE AND LEAF TOPOLOGY

When architecting layer 2, consider:

- Hardening port configurations and spanning tree
- Failure domains and blast radius
- Changing control needs
- Overall scale target
- SLA and performance objectives
- Maximum acceptable downtime

Strategies:

- Use spine/leaf for scale-out
- Reduce failure domains
- Segment change control
- Overprovision capacity
- Meet SLAs through redundancy
- Eliminate single points of failure



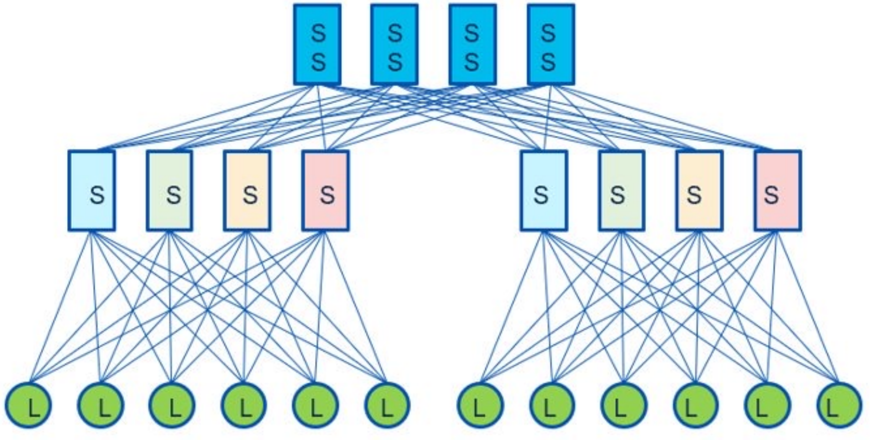
Knight Shift IT
Secure. Reliable. Automated.

SECURING LAYER 2:

CONSIDER SPINE AND LEAF ARCHITECTURE WITH SUPER-SPINE TOPOLOGY

Reducing the impact of failure domain:

- Deploy layer 3 where you can and layer 2 where you have to
- Use your ToR or Leaf as server gateway, deploy iBGP as your IGP in the context of leaf as gateway for servers



3 Tier Leaf-Spine-Super Spine

KNIGHT SHIFT IT
Secure. Reliable. Automated.

STEP 3

STRENGTHEN THE NETWORK CORE: REVIEW YOUR IGP PROTOCOLS

STRENGTHENING THE NETWORK CORE

- Securing the heart of the network infrastructure requires a wholistic approach from at all 7 Layer of OSI model
- Enhancing IGP scalability by phasing out OSPF and EIGRP for growing networks. iBGP is a good starting point.
- To withstand DDoS attacks, the Implementing redundancy and failover in the core is a must for uninterrupted service.
- Advanced network segmentation. Isolating sensitive data and services.
- Robust firewall deployment and intrusion prevention strategies.
- Traffic engineering: Managing data flows for optimal performance.

KNIGHT SHIFT IT
Secure. Reliable. Automated.

STEP 4

SECURE YOUR LAYER 3 DOMAIN

PHASE OUT IGP LIMITATIONS IN YOUR CORE

SECURING LAYER 3

Why BGP for the Core?

- OSPF limited to 10K routes
- EIGRP instability over 20K routes
- Random IGP flaps = multi-hour outages

BGP Advantages

- Proven scaling into millions of routes
- Stability through best practices
- Advanced traffic engineering

Key Takeaways:

Leverage BGP’s scalability while applying filters and controls.

Best Practices

- Set max prefix on edge routers
- no bgp fast-external-fallover is your friend when you bump a cable
- Apply max prefix on Upstream IP links - neighbor 216.x.x.X maximum-prefix 995000 98 restart 2
- Limit inbound prefix filters for IXP links in the 1000s

- Prefix filters and AS_PATH filters
- Route reflection for control plane

KNIGHT SHIFT IT

Secure. Reliable. Automated.

SECURING LAYER 3:
BEST PRACTICES

- Boundaries are first line of defence against DDoS
- Set max prefix on edge routers with eBGP
- Prefix filters and AS_PATH filters
- Introduce Route reflection for control plane

Case Study: Telco Outage 2023

- Edge router missing max prefix limit
- Accepted unchecked routes
- Exceeded capacity, control plane failure
- Multi-hour, nationwide outage

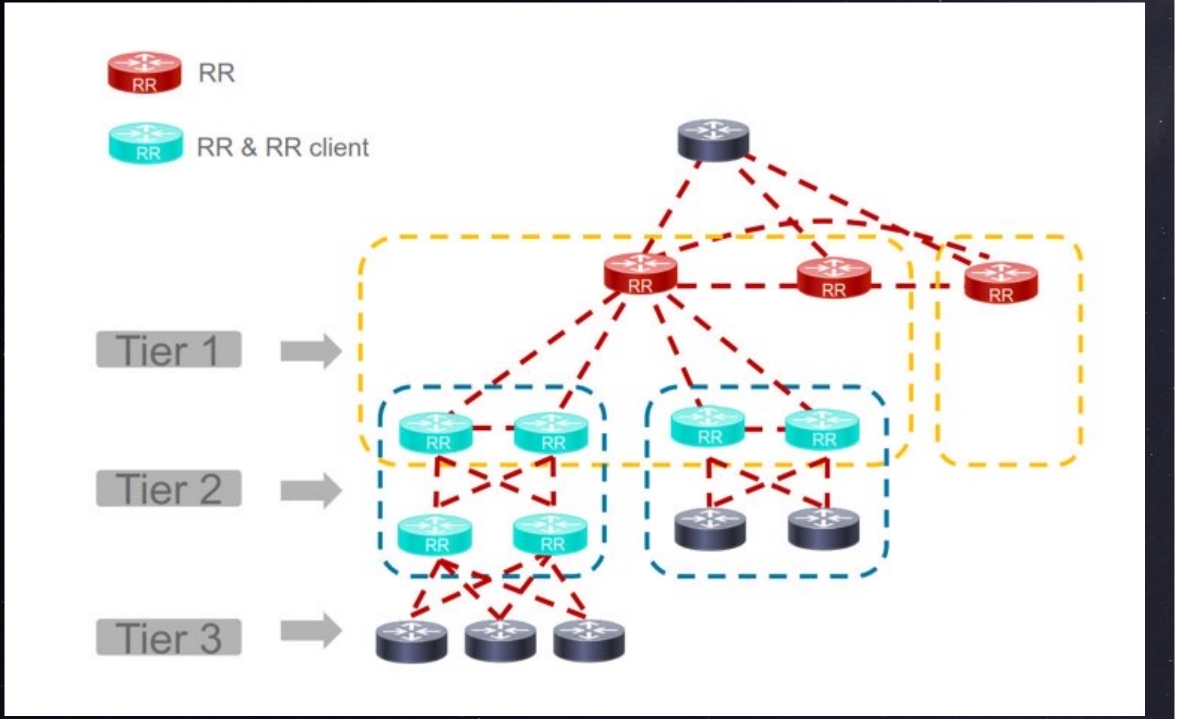
In short: Leverage BGP’s scalability while applying filters and controls.

KNIGHT SHIFT IT
Secure. Reliable. Automated.

SECURING LAYER 3:

SCALING BGP WITH HIERARCHICAL ROUTE REFLECTORS

- Chain RRs to keep the full mesh between RRs and non-clients small
- Make RRs clients of other RRs
- RR is both an RR and RR client
- iBGP topology should follow physical topology
- Prevents suboptimal routing, blackholing and routing loops
- RRs in top tier need to be fully meshed
- No limit to the amount of tiers



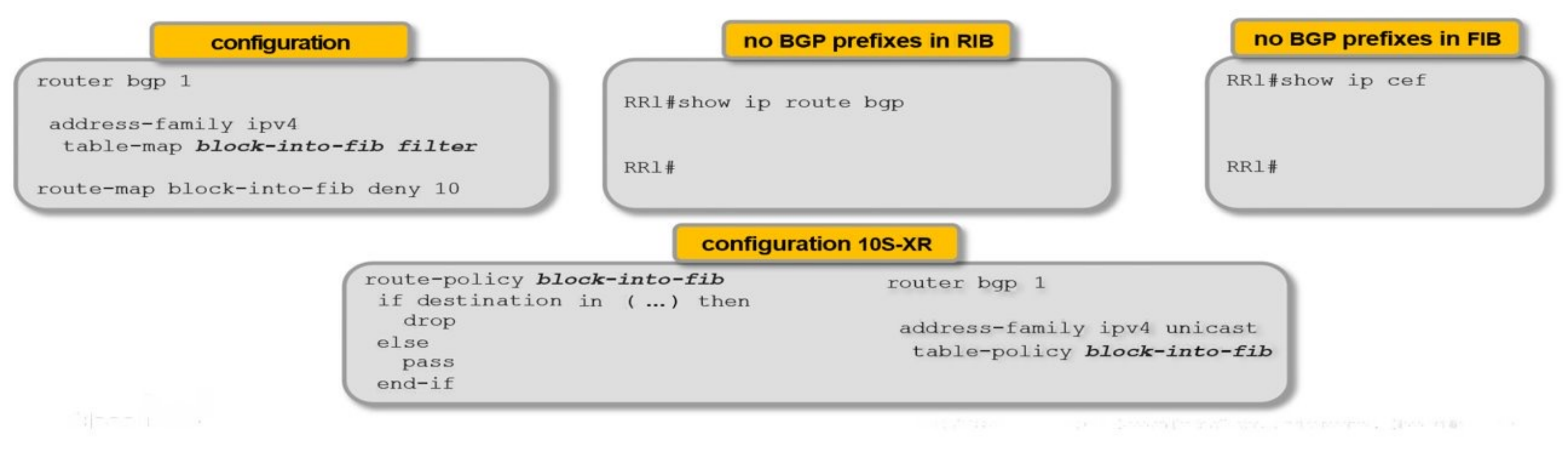
KNIGHT SHIFT IT

Secure. Reliable. Automated.

SECURING LAYER 3:

BGP RR SCALE - SELECTIVE RIB DOWNLOAD

- To block some or all of the BGP prefixes into the RIB (and FIB)
- Only for RR which is not in the forwarding path
- Saves on memory and CPU
- Implemented as filter extension to table-map command



configuration

```
router bgp 1

 address-family ipv4
  table-map block-into-fib filter

route-map block-into-fib deny 10
```

no BGP prefixes in RIB

```
RR1#show ip route bgp


RR1#
```

no BGP prefixes in FIB

```
RR1#show ip cef


RR1#
```

configuration 10S-XR

```
route-policy block-into-fib
 if destination in ( ... ) then
   drop
 else
   pass
 end-if
```

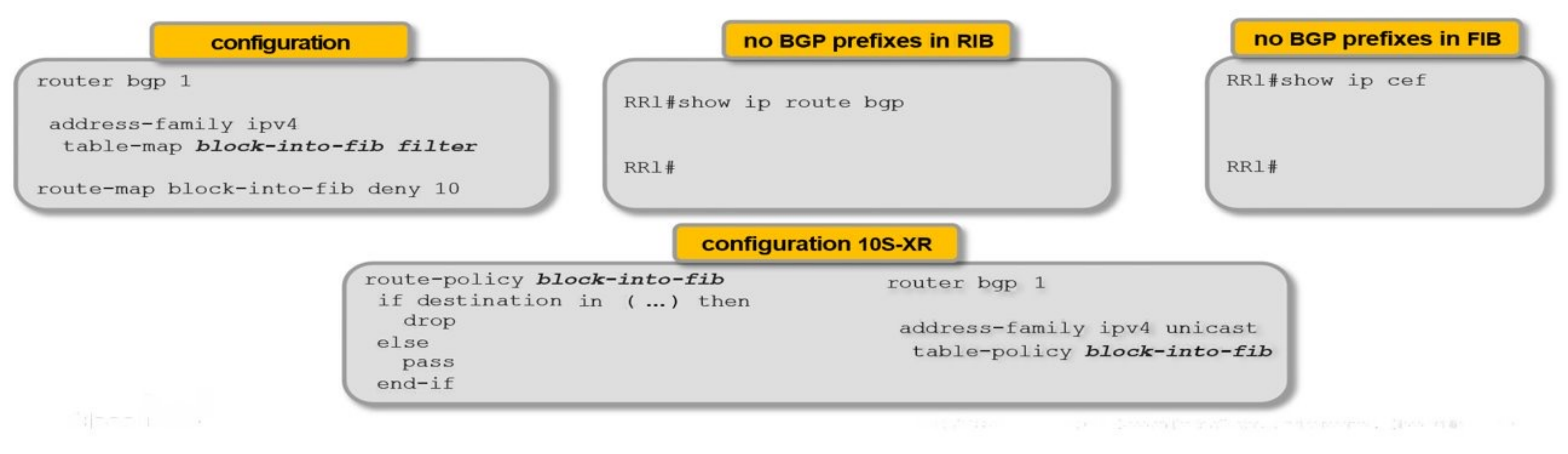
```
router bgp 1

 address-family ipv4 unicast
  table-policy block-into-fib
```

KNIGHT SHIFT IT
Secure. Reliable. Automated.

SECURING LAYER 3:

BGP RR SCALE - SELECTIVE RIB DOWNLOAD

- Ipv4/ipv6 family
- Not needed for AFs vpnv4/6
- ASR1 k testing indicated 300% of RR client session scaling (in order of 1000s)



configuration

```
router bgp 1

 address-family ipv4
  table-map block-into-fib filter

route-map block-into-fib deny 10
```

no BGP prefixes in RIB

```
RR1#show ip route bgp


RR1#
```

no BGP prefixes in FIB

```
RR1#show ip cef


RR1#
```

configuration 10S-XR

```
route-policy block-into-fib
 if destination in ( ... ) then
   drop
 else
   pass
 end-if
```

```
router bgp 1

 address-family ipv4 unicast
  table-policy block-into-fib
```

STEP 5

MANAGING DATA FLOWS FOR OPTIMAL PERFORMANCE

MANAGING DATA FLOWS:

OPTIMISING TRAFFIC FLOWS

Challenges:

- Securing North-South traffic
- Isolating sensitive East-West traffic
- Maintaining integrity of addresses

Strategies:

- ACLs & VRFs for fine-grained control
- Consistent policy enforcement
- AI/ML for predictive analytics

Outcomes:

- Securing North-South traffic
- Balance security and efficiency
- Meet performance SLAs
- Detect anomalies proactively

KNIGHT SHIFT IT
Secure. Reliable. Automated.

MANAGING DATA FLOWS:

DDOS MITIGATION WITH BGP FLOWSPEC

- Single point of control to program rules in many clients
- Granularity allows a very precise description/matching of the attack traffic
- Can be used for both mitigation and diversion of the attack traffic without impacting the flow of the rest of the traffic targeted to the victim
- Off-Load Mitigation system: Filtering stateless attacks on the edge route
- Permits mitigation of millions of PPS of dirty traffic while liberating precious CPU cycles on the scrubbing device for more advanced mitigation needs

MANAGING DATA FLOWS:

STRATEGIC DDOS DEFENCE FRAMEWORK

Detection and Analysis:

- Log analysis for operational intelligence
- Integrate threat reputation feeds

Mitigation Technologies:

- BGP FlowSpec for surgical traffic control
- Anycast POPs to drop traffic at source
- RTBH filtering near attack source

Automation:

- Auto-block and release with reputation
- FlowSpec integrated with Anycast

Optimisation:

- Regular testing for seamless failover
- Tuning for precision attack matching

Outcomes:

- Meet performance SLAs
- Detect anomalies proactively

KNIGHT SHIFT IT
Secure. Reliable. Automated.

DDOS MITIGATION APPROACHES

- Multiple models for diverting and scrubbing attack traffic
- Depends on network topology and protocols
- Common tactics:
  - Divert attack traffic to scrubbing devices
  - Analyse packets to filter malicious vs good
  - Re-inject good traffic
  - Route bad traffic to black hole

- Hybrid models utilized in large networks:
  - Anycast for distributed scrubbing
  - BGP FlowSpec for surgical traffic control

DEPLOY BGP FLOW SPEC FOR DDOS MITIGATION

- Single point of control to program rules in many clients
- Granularity allows a very precise description/matching of the attack traffic
- Supports IPv4/IPv6
- Can be used for both mitigation and diversion of the attack traffic without impacting the flow of the rest of the traffic targeted to the victim
- Off-Load Mitigation system: Filtering stateless attacks on the edge route
- Permits mitigation of millions of PPS of dirty traffic while liberating precious CPU cycles on the scrubbing device for more advanced mitigation needs

Action Plan for Global DDoS Defense Using BGP Flowspec, Anycast, and RTBH

Strategic DDoS Defense Framework

Detection & Analysis

- Log analysis for operational intelligence
- Integrate threat reputation feeds

Mitigation Technologies

- BGP FlowSpec for surgical traffic control
- Anycast POPs to drop traffic at source
- RTBH filtering near attack source

Automation

- Auto-block and release with reputation
- FlowSpec integrated with Anycast

Automation

- Auto-block and release with reputation
- FlowSpec integrated with Anycast

Optimization

- Regular testing for seamless failover
- Tuning for precision attack matching

Outcomes

- Agile global attack absorption
- Minimize customer impact
- Carrier-grade backbone resilience

KNIGHT SHIFT IT
Secure. Reliable. Automated.

FINAL THOUGHTS

FINAL THOUGHTS

- **Staying Ahead of Emerging Threats**
  - Staying ahead of evolving cyber threats is not optional - it's essential. Continual adaptation and embracing new technologies keeps organizations a step ahead rather than merely reacting to attacks. Proactive vigilance and preparation provide robust safeguards against emerging risks before they escalate.
- **Commitment to Continuous Improvement**
  - The path to robust network security is one of ongoing improvement. It's a commitment to continuously evolving our strategies, learning from new challenges, and adapting to the ever-changing digital landscape.
- **Advancements in AI and Machine Learning**
  - We delved into the revolutionary impact of AI and machine learning – from automating log analysis to proactive threat detection and intelligent management of IP addresses. These technologies are not just enhancements; they are essential in our evolving cybersecurity landscape.

KNIGHT SHIFT IT
Secure. Reliable. Automated.

FINAL THOUGHTS CONT…

- **Fostering ISP Synergy**
  - Encourage ISPs of all sizes to engage in direct peering and intelligence sharing - especially regarding the deployment and optimization of BGP Flowspec to strengthen the global network defence.

- **Invitation for Collaboration and Feedback**
  - Finally, this journey is not one to be walked alone. We invite collaboration, feedback and shared experiences. Together we can forge a path towards more resilient, secure and advanced networks.

Thank you!

Do you have any questions?

ahad@knightshiftit.com.au

Mobile: +61 478 509 000
Office: +61 2 9159 9194

https://www.knightshiftit.com.au

KNIGHT SHIFT IT
Secure. Reliable. Automated.