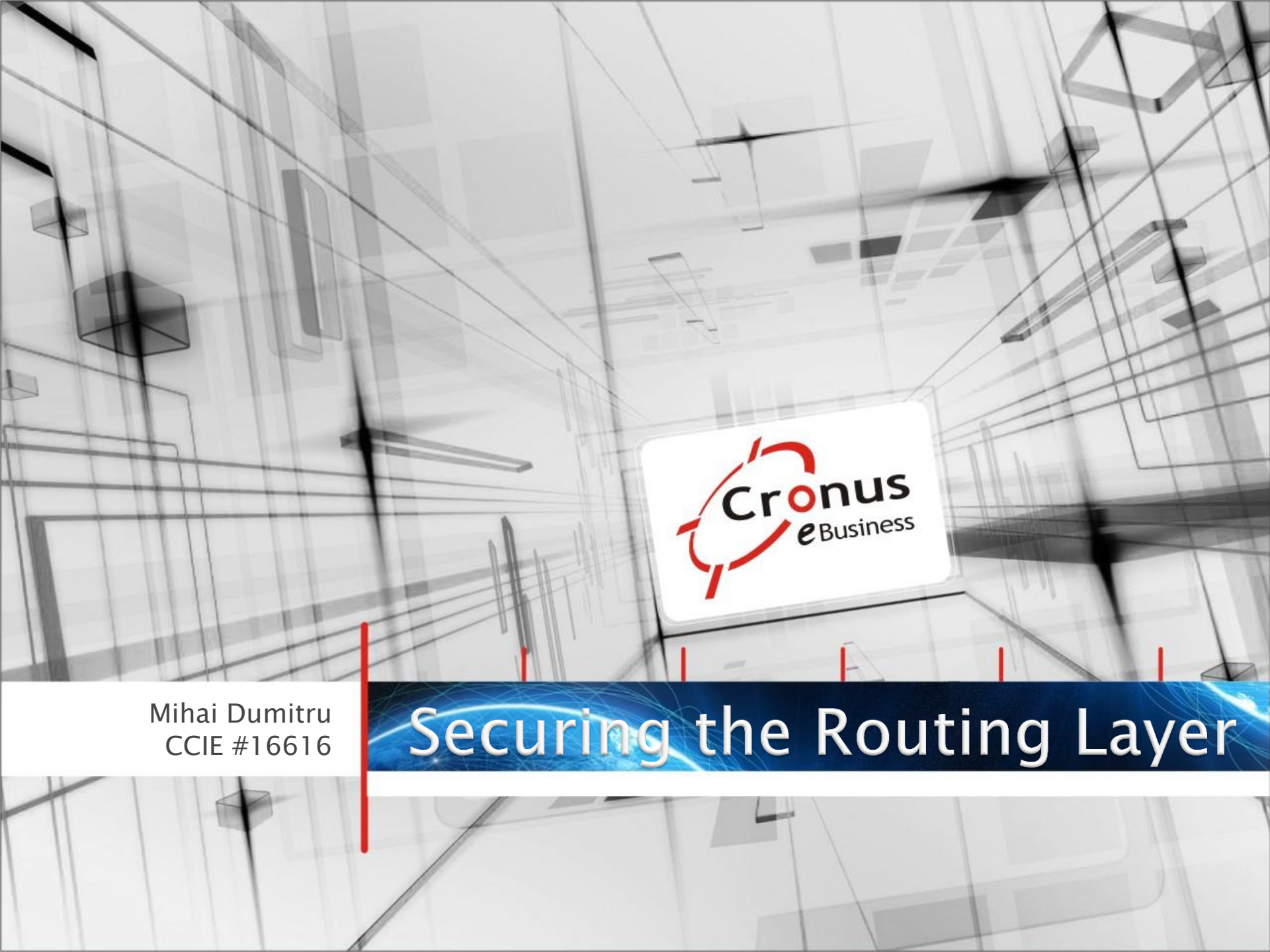


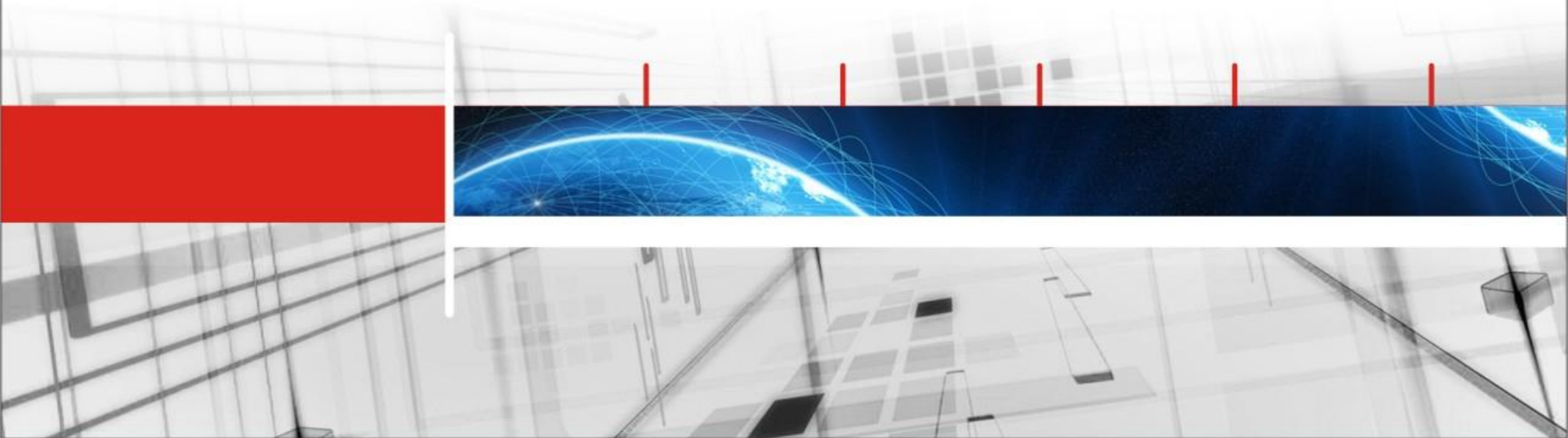
Mihai Dumitru
CCIE #16616

Securing the Routing Layer

- Sophisticated (read expensive) security layers are sometimes deployed on top of a bad routing layer…
- Sometimes it is even possible to get in undetected
- We will take a look at some examples.

Take 1

IPv4 First Hop Security



DHCP Snooping

```
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping

interface Port-channel1
 ip dhcp snooping trust
```

or

```
ip dhcp snooping vlan 10
ip dhcp snooping

interface Vlan10
 ip helper-address <DHCP server>
 ip helper-address <ISE server>
```

- Mitigates the risk of DHCP starvation (followed by DHCP spoofing, for example, in order to inject false DNS information)
- Is required for Dynamic ARP Inspection to work

FHRP Configuration

```
interface Vlan10
 ip address 10.128.10.11 255.255.255.0
 standby 10 ip 10.128.10.1
 standby 10 timers msec 200 msec 600
 standby 10 priority 105
 standby 10 preempt
 standby 10 authentication HSRP_KEY
 standby 10 track 1
```

- Something wrong?

FHRP Authentication

```
interface Vlan10
 ip address 10.128.10.11 255.255.255.0
 standby 10 ip 10.128.10.1
 standby 10 timers msec 200 msec 600
 standby 10 priority 105
 standby 10 preempt
 standby 10 authentication HSRP_KEY
 standby 10 track 1
```

- Plain text authentication merely used to change the default from ‘cisco’
- Can be sniffed, then used to setup a MITM attack, for example

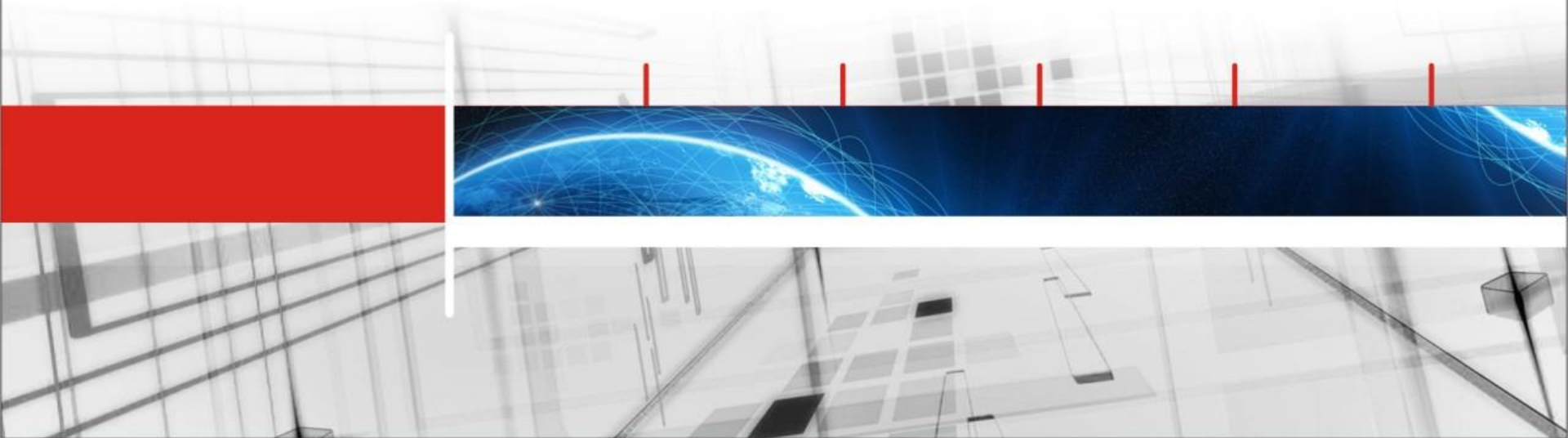
FHRP Authentication

```
key chain HSRP_KEY
 key 0
  key-string <removed>

interface Vlan10
 ip address 10.128.10.11 255.255.255.0
 standby 10 ip 10.128.10.1
 standby 10 timers msec 200 msec 600
 standby 10 priority 255
 standby 10 preempt
 standby 10 auth md5 key-chain HSRP_KEY
 standby 10 track 1
```

- Either increase **priority** to 255 or configure MD5 **hash** authentication or both

Take 2

Basic Routing Configuration



Basic Routing Configuration

```
router eigrp 100
 network 10.16.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel0

router ospf 100
 network 10.16.0.100 0.0.0.0
 passive-interface default
 no passive-interface Tunnel0

router rip
 network 10.0.0.0
 passive-interface default
 no passive-interface Tunnel0
 version 2
```

- What's the big deal?

Basic Routing Configuration

```
router eigrp 100
 network 10.16.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel0

router ospf 100
 network 10.16.0.100 0.0.0.0
 passive-interface default
 no passive-interface Tunnel0

router rip
 network 10.0.0.0
 passive-interface default
 no passive-interface Tunnel0
 version 2
```

- The passive-interface configuration prevents routing adjacencies with EIGRP and OSFP
- Even though RIP will not advertise any prefix out of a passive interface, *it will learn specific* prefixes, making traffic hijacking possible
- RIP still used with very large hub-and-spoke networks

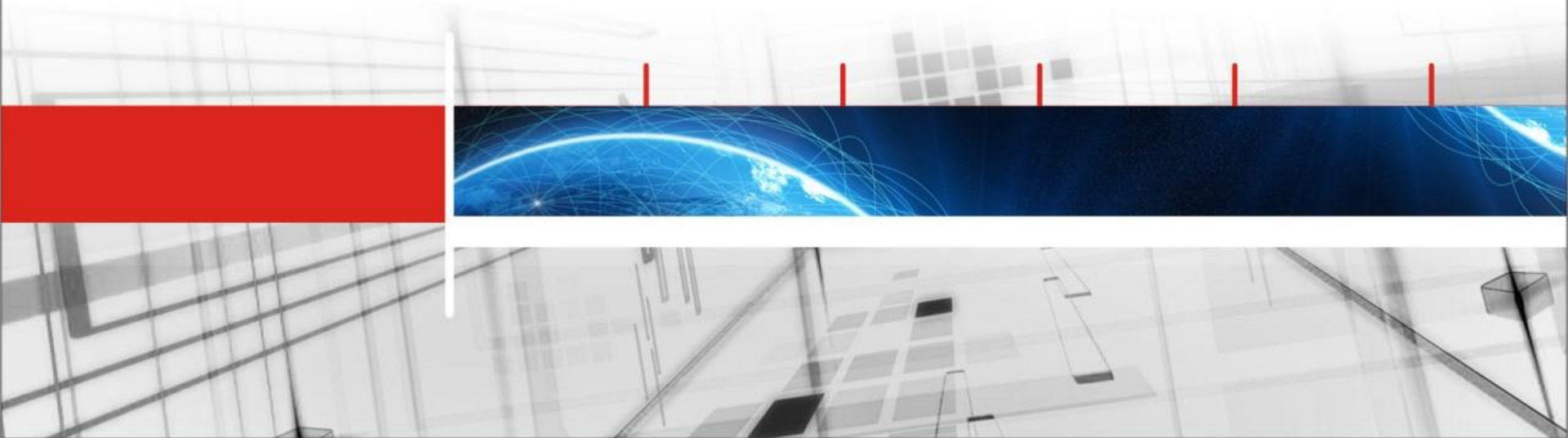
Basic Routing Configuration

```
key chain no-RIP
 key 0
  key-string <garbage>

interface GigabitEthernet0/0/3
 description --3G
 ip rip authentication mode md5
 ip rip authentication key-chain no-RIP

router rip
 network 10.0.0.0
 passive-interface default
 no passive-interface Tunnel0
 version 2
```

- Although RIPv2 is classless, the configuration of the RIP process is still classful
- Non-participating interfaces may belong to the same class
- In this case, configure authentication *on the non-participating interfaces,* as well

Take 3

DMVPN Security



DMVPN Security

```
crypto isakmp policy 10
 encr aes 256
 hash sha384
 authentication pre-share
 group 15
 lifetime 1800
crypto isakmp key <key> address 0.0.0.0

crypto ipsec profile DMVPN
 set transform AES256-SHA384-TRANSP

interface Tunnel0
 ip authentication mode eigrp 100 md5
 ip authen key-chain eigrp 100 EIGRP_KEY
 ip nhrp authentication <removed>
 tunnel protection ipsec profile DMVPN
```

- DMVPN over the Internet usually used as a backup tunnel (MPLS VPN as primary path)
- Pretty typical DMVPN hub configuration – err, maybe with inadequate cypher suite
- Something wrong?

DMVPN Security

```
crypto isakmp policy 10
 encr aes 256
 hash sha384
 authentication pre-share
 group 15
 lifetime 1800
crypto isakmp key <key> address 0.0.0.0

crypto ipsec profile DMVPN
 set transform AES256-SHA384-TRANSP

interface Tunnel0
 ip authentication mode eigrp 100 md5
 ip authen key-chain eigrp 100 EIGRP_KEY
 ip nhrp authentication <removed>
 tunnel protection ipsec profile DMVPN
```

- Yes, we can actually establish a rogue tunnel to the hub, if we knew the keys
- Pre-configured keys must be the same for spoke-to-spoke, and they probably never get changed
- And quite many people could have had access to a spoke router configuration file (contractors, especially)

DMVPN Security

snmp-server community <removed> **RW**

- Could it be worse?
- With SNMP running, we don't even need a CLI username and password combination
- SNMP ACL you say? We can spoof the source address, no problem (SNMP is UDP based)
- Possibly get in undetected? Change configs for fun?

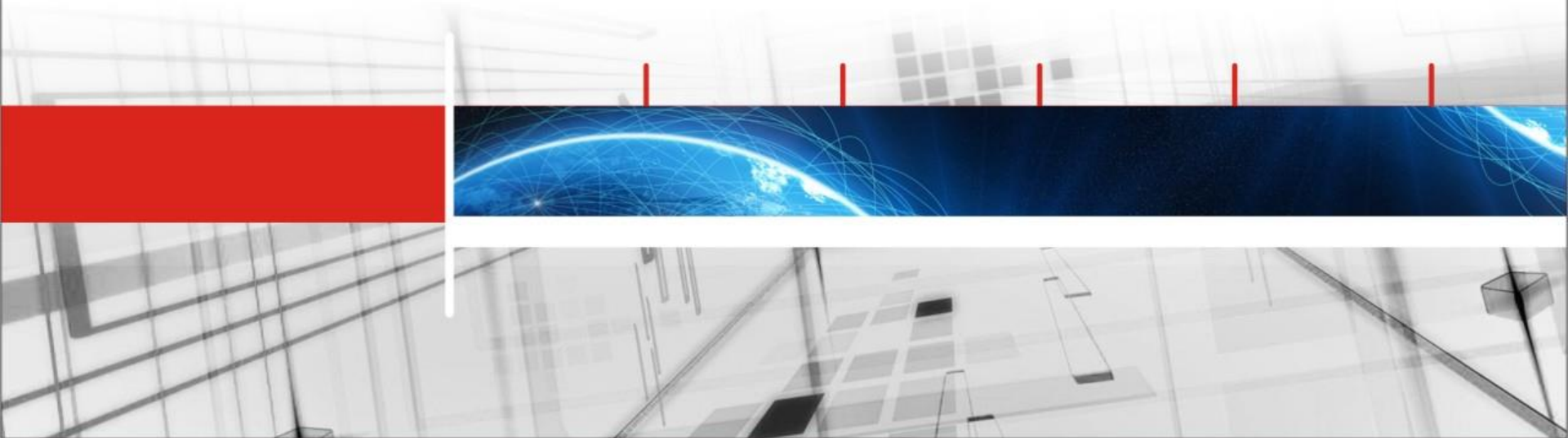
DMVPN Security

```
object-group network DMVPN_PEERS
 host <spoke1>
 host <spoke2>

ip access-list extended DMVPN_ACL
 permit udp object-group DMVPN_PEERS
eq isakmp any eq isakmp
 permit esp object-group DMVPN_PEERS
any

interface GigabitEthernet0/0
 ip access-group DMVPN_ACL in
```

- Need to configure infrastructure ACL on the hub (not necessarily on the spokes, because of the static NHRP mapping)
- Need to configure SNMPv3
- iWAN: separate the Internet routing table from the internal routing table (F-VRF Front Door VRF)

Take 4

BGP Security



BGP Configuration

```
router bgp 65500
 bgp log-neighbor-changes
 network 9.128.255.0 mask 255.255.255.0
 neighbor 9.0.0.7 remote-as 1234
 neighbor 9.0.0.7 timers 10 30
 neighbor 9.0.0.7 send-community
 neighbor 9.0.0.7 route-map BGP-IN in
 neighbor 9.0.0.7 route-map BGP-OUT out
```

- BGP relies on TCP as transport protocol
- Peer IP address revealed by traceroute (unless RFC1918 address or multi-hop BGP session with a Loopback address)
- What if we send multiple TCP resets with a spoofed source?

BGP Configuration

```
router bgp 65500
 bgp log-neighbor-changes
 network 9.128.255.0 mask 255.255.255.0
 neighbor 9.0.0.7 remote-as 1234
 neighbor 9.0.0.7 timers 10 30
 neighbor 9.0.0.7 send-community
 neighbor 9.0.0.7 route-map BGP-IN in
 neighbor 9.0.0.7 route-map BGP-OUT out
 neighbor 9.0.0.7 ttl-security hops 1
```

- GTSM: the TTL value is set to 255 rather than 1, and a "minimum TTL-value" is enforced
- Private peer IP addresses or ebgp-multihop (with loopbacks)
- Infrastructure ACL
- MD5 hash authentication is *CPU intensive*

Take 5

IPv6 Concerns

Source: BRKSEC-2003

Dual Stack with IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite firewall...
  - IPv6 is enabled by default (Windows, Linux, Mac OS/X)
- Your network:
  - *Does not run IPv6*
- Your assumption: I'm safe
- How much safe?

Dual Stack with IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite firewall...
  - IPv6 is enabled by default (Windows, Linux, Mac OS/X)
- Your network:
  - *Does not run IPv6*
- Your assumption: I'm safe

- Reality: you are not safe
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack
- IPv6 vulnerability scanning must be done for both IPv4 and IPv6 *even in an IPv4-only network*

Can We Block Rogue Tunnels?

- Rogue tunnels by naïve users:
  - Sure, block IP protocol 41 and UDP/3544, UDP/3074
  - In Windows: disable 6to4, isatap, teredo
- *In reality, no easy way to detect really rogue tunnels*
- Configuring native IPv6 firewalls and IPS is probably a better alternative
- Or disable IPv6 on Windows through registry
  - HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponents

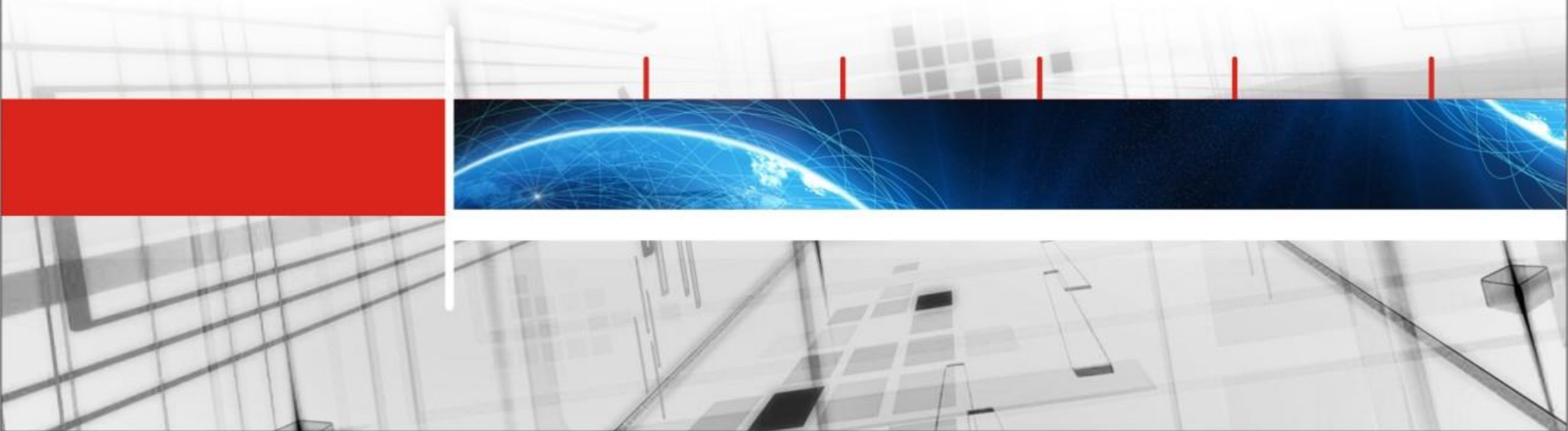
Is IPv6 in My Network?

- Look inside NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
  - ICMPv6 Packets, especially RA
- Check your IPS system for discovery of ICMPv6 traffic
- Look into DNS server log for resolution of ISATAP & Microsoft Teredo servers

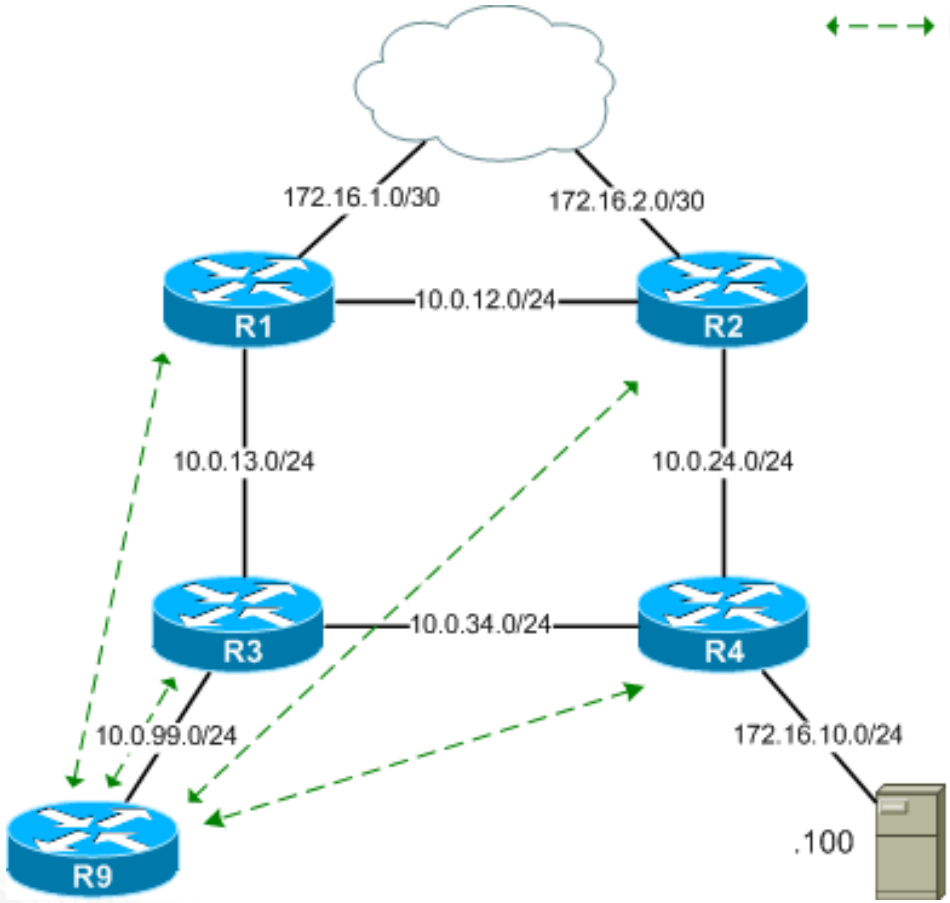
Routing as Security Tool

Remotely Triggered Black Hole

Example network from: PacketLife



Remotely Triggered Black Hole



- Routers R1-R4 are the network core. Router R9 is an off-path BGP router for route injection
- OSPF runs across the core to exchange internal routes
- The server attached to R4 was compromised

Cronus eBusiness

Remotely Triggered Black Hole

R1-4:
ip route **192.0.2.1** 255.255.255.255 **Null0**

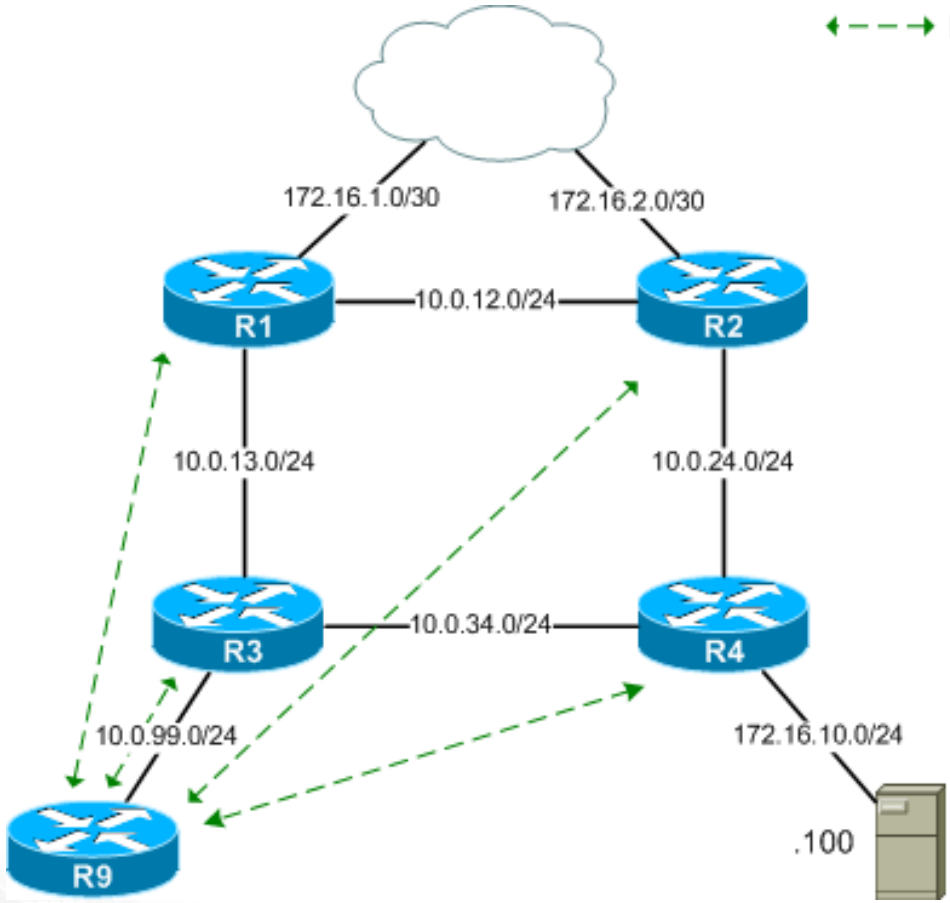
R9:
route-map RTBH
 match **tag 666**
 set ip next-hop **192.0.2.1**
 set origin igp
 set community no-export

router bgp 65100
 redistribute static route-map RTBH

ip route 172.16.10.100 255.255.255.255 Null0 tag 666

- RTBH works by injecting specially-crafted BGP routes into the network, forcing routers to drop all traffic with a specific next-hop -- effectively creating a "black hole."
- It is enough to configure a static route on R9

Remotely Triggered Black Hole

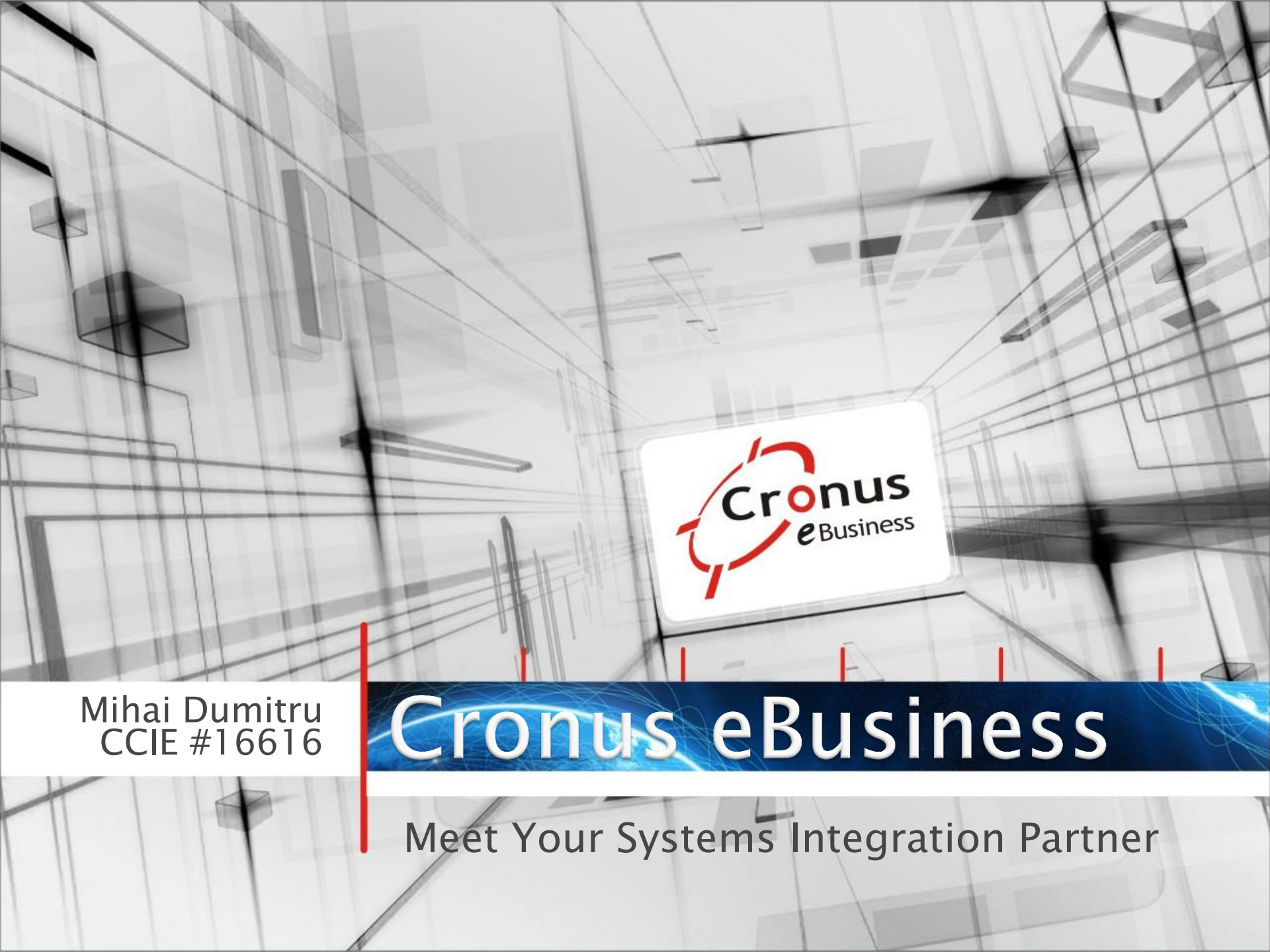


- Now take a look at this picture again.

- *What if:*
- R9 was a server and
- it was able to automatically fetch lists of known malware sites (C&C sites),
- resolve names into IP addresses and
- install all the RTBH routes for us?

Conclusions

- Expensive security layers ruined by bad routing configuration. The most common risks are denial of service and traffic hijacking.
- Pick the low-hanging fruit first: fix the existing configuration. Or, on the contrary, leverage routing as a security tool.
- See the whole picture
- Check your infrastructure. Ask Cronus for a (possibly free) assessment!



Mihai Dumitru
CCIE #16616

Cronus eBusiness

Meet Your Systems Integration Partner