TOMORROW
starts here.

Cisco Connect
Praha, Česká republika
24.–25. 3. 2015
Budujeme bezpečný perimetr sítě

TECH-SEC: Building an Highly Secure Internet Edge

Gaweł Mikołajczyk
gmikolaj@cisco.com
Security Technical Solutions Architect
CCIE #24987, CISSP-ISSAP, CISA, C|EH, SFCE
Agenda

- Internet Edge Building Blocks
- Protecting the Internet Peering
- Firewall Deployment and Segmentation
- Next-Generation Firewall
- Web Security and Content Filtering
- Next-Generation IPS
- SSL Decryption
- Email Security
- Advanced Malware Protection
- Identity for User Attribution
- Network Forensics with Cyber Threat Defense
- Incident Response Detection and Mitigation
- Open Source and Custom Tools
Session Timeline as a Maturity Model


SSL Decryption and Inspection → Email Security → Advanced Malware Protection (AMP) → Identity Attribution → Network Forensics → Incident Response → Open Source Custom Tools

Where is my Organization on the adoption trajectory?
“Configuration is only half the story.

This presentation is about the other half.”

Bruce Schneier
Security Guru
About the Speaker

- Security Technical Solutions Architect, 8¾ years at Cisco
- Based in Warsaw, Poland
- Graduated in Telecommunications
- Long time Cisco Networking Academy Instructor
- Cisco Live! Speaker since 2012 London

Gaweł Mikołajczyk
gmikolaj@cisco.com
@gapheu
/gawelmikolajczyk
Internet Edge Security Building Blocks
Revisiting the Past – Smart Business Architecture (SBA)
Full Internet Edge and WAN Edge Topology
„The problem is the THREATS. “

Martin Roesch
VP, Chief Security Architect
SOURCEfire Founder
Snort Creator
Threat-Centric Security Approach

- The problem is the THREATS.

  BRKSEC-2135 The Importance of Threat-Centric Security

- What high value assets am I trying to protect?
  - Intellectual property, customer and employee data,
  - Network and compute infrastructure

- What are the possible threats?
  - Internal and External, Structured and Unstructured

- How do I detect and mitigate the threats?
  - This is what this session is about at the Internet Edge

- What is my incident response approach?
  - Will I just sit there or clean up my environment?
Internet Edge Connectivity Peering
Internet Edge – Peering

The Fatal Assumptions:

1. My network is **physically secure**
   - Device access under control

2. I understand my network
   - Dealing with Infrastructure Complexity

3. My **protocols are secure**
   - Management, Control and Data Planes

4. I **know my attacker**
   - Target and motives, DDoS protection

5. I **know what to do**
   - Operationalizing Attack Mitigation
"Why Would Anyone Hack Into My Router?"

PBR1: from PC to Server → Next hop tunnel

PBR2: from Server to PC → Next hop tunnel

BRKSEC-2345 Critical Infrastructure Protection (2013 London)
Physical Security Principles and Procedures

- **Can detect takeover of device**
  - MUST detect login of authorised admin
  - MUST detect brute force SSH attacks
  - MUST detect password recovery
  - MUST detect device replacement (UDI)
  - MUST check device integrity regularly
    - OS, configuration, file system

- **Cannot detect wiretap**
  - MUST protect all control plane protocols (BGP, IGP, LDP)
  - MUST protect all management plane protocols (SSH, SNMP)
    - Only data plane attacks are possible

- **After each reboot**, link-down event, etc:
  - Device could have been replaced
  - Password recovery could have been done
  - Check system:
    - Unique Device Identifier (UDI), OS, configuration, enable password

- **After unexpected login** from admin:
  - Change password for that admin
  - Check system
    - OS, configuration, enable password

- **Regularly** (ex: once in 24h)
  - Check system:
    - OS, configuration, enable password
Device Software Authenticity Challenges Today

Configuration
- Misconfiguration
- Lacking security
- Sabotage

OS
- Protocol vulnerability
- OS vulnerability
- Rootkit

Boot ROM
- Physical attacks

Unique Device Identifier (UDI)
- Physical attacks
Device Software Authenticity Outlook for the Future

- **Configuration with Checksum**: Verifies first, then uses
- **OS with Vendor Signature**: Checks OS correctness, boots

**Physically Secure**

- **Boot ROM**
  - SUDI allows for globally unique, secure device identification
    - Cannot replace device
  - **Boot process secured**
    - Cannot modify Boot ROM
    - Cannot modify OS
  - Secure OS coding practices
    - CSDL Practices
    - Reduces vulnerabilities
  - Upgrade procedures

Verifying Software Authenticity on ASA

Available in 9.3(2) Software Release. Display digital signature information related to software authentication for a specific image file with `show software authenticity running` command in privileged EXEC mode. The output provides:

- **Name of the filename in memory.**
- **Type of image being shown.**
- **Signature information**, includes the following:
  - common name, name of the software manufacturer.
  - organization unit, hardware that the software image is deployed on.
  - organization name, which is the owner of the software image.
- **Certificate serial number**, which is the certificate serial number for the digital signature.
- **Hash algorithm**, which indicates the type of hash algorithm used in digital signature verification.
- **Signature algorithm**, which identifies the type of signature algorithm used in digital signature verification.
- **Key version**, which indicates the key version used for verification.

```
asa5506-X# show software authenticity running
Image type : Development
Signer Information
  Common Name : abraxas
  Organization Unit : NCS_KentonASA
  Organization Name : CiscoSystems
  Certificate Serial Number : 5448091A
  Hash Algorithm : SHA2 512
  Signature Algorithm : 2048-bit RSA
  Key Version : A

Verifier Information
  Verifier Name : ROMMON
  Verifier Version : Cisco Systems ROMMON, 1.0.16

ROMMON Trust Anchor
```

```
ASAv# show software authenticity running
Image type : Release
Signer Information
  Common Name : abraxas
  Organization Unit : ASAv
  Organization Name : CiscoSystems
  Certificate Serial Number : 5476833D
  Hash Algorithm : SHA2 512
  Signature Algorithm : 2048-bit RSA
  Key Version : A
```
Is Your Network Physically Secure?

- **Cannot guarantee** physical security
- Password recovery, device replacement, sniffing, wiretaps, man-in-the-middle

- Secure Management and Control Planes
- Secure Data Plane (IPsec)
- Monitor for device changes (**reload**)
- Check UDI (**sh license udi**)
- Check device config correctness
- Procedures to **isolate an intruded device**
- Procedures to **re-gain control** of a physically intruded device
IOS Hardening Best Practices

- Cisco Guide to Harden Cisco IOS Devices
  - Secure **Operational Procedures**
    - Monitor Security Advisories
    - Leverage AAA, Centralize Log Collection
    - Use Secure Protocols when possible
  - **Management Plane** (SSH, SNMP, NetFlow)
    - Disable unused Services, Password Security
    - Secure Management Sessions
    - Thresholding for Memory, CPU, Leaks
    - Management Plane Protection (MPP)
  - **Control Plane** (ICMP, BGP, RSVP)
    - Control Plane Policing (CoPP), Protection (CPPr), HW Rate-Limiters
  - **Data Plane** (production traffic)
    - Antispoofing with uRPF, IPSG, Port Security, DAI, ACLs
    - Traffic Access Control

I understand my network. A Cisco Example.

- Offices in 100+ countries
- 15 Billion Flows per day
- 125,000 endpoints (with laptops and phones)
- 150,000+ servers of all types
- 40,000 routers
- 1,500 labs
- 350 IPS Sensors / 1.5M Alerts per day
- 12 major Internet POPs
- One CSIRT analyst for every 7,000 employees
„Soon, it will not be feasible to directly configure routers”

Michael Behringer
Distinguished Engineer
Autonomic Networking Pioneer
My Protocols are Secure
BGP Prefix Highjacking
Before 24th Feb’08 (UTC):

AS36561 (YouTube) announces 208.65.152.0/22.
24th Feb’08, 18:47 (UTC):
AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. PT’s upstream provider AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
24TH Feb’08, 21:23 (UTC):
AS36561 has been announcing 208.65.153.0/24 since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to AS36561

http://www.ripe.net/news/study-youtube-hijacking.html
BGP Secure InterDomain Routing (SIDR)

- Validation between Enterprise and Provider is important, BGP relies on a transitive trust model
- BGP Speaker queries the Validated Prefix Database, downloaded from the Cache Server
- Resource Public Key Infrastructure (RPKI) cache servers perform BGP Prefix Authentication
- BGP Speaker ensures the prefix originated from the expected AS
Utilizing SIDR – Valid, Unknown, Invalid Routes

router bgp 64726
  bgp always-compare-med
  bgp log-neighbor-changes
  bgp deterministic-med
  no bgp default ipv4-unicast
  bgp rpki server tcp 217.193.137.117 port 30000 refresh 60
  bgp rpki server tcp 2001:918:FFF9:0:250:56FF:FE15:159 port 8282 refresh 60
  bgp rpki server tcp 2001:918:FFF9:0:250:56FF:FE15:159 port 30000 refresh 60
  bgp rpki server tcp 217.193.137.117 port 8282 refresh 600
  neighbor 2001:428:7000:A:0:1:0:1 remote-as 64209

ASR#show bgp sum
BGP router identifier 66.77.8.142, local AS number 64726
BGP table version is 11688639, main routing table version 11688639
Path RPKI states: 38286 valid, 1574331 not found, 4558 invalid
404300 network entries using 59836400 bytes of memory
1617175 path entries using 103499200 bytes of memory

RFC 6810 The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6811 BGP Prefix Origin Validation
I know my attacker, He is DDoSing me right now

More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack
By Daniel Cid on March 10, 2014 • 36 Comments

Distributed Denial of Service (DDoS) attacks are becoming a common trend on our blog lately, and that’s OK because it’s a very serious issue for every website owner. Today I want to talk about a large DDoS attack that leveraged thousands of unsuspecting WordPress websites as indirect source amplification vectors.

Worst DDoS attack of all time hits French site

Summary: A website in France was hammered on Monday by a Distributed Denial of Service attack that hit it at a rate from 340Gbps to 400Gbps making it the strongest DDoS attack ever.

By Steven J. Vaughan-Nichols for Networking | February 13, 2014 — 21:50 GMT (13:50 PST) Follow Steven

Get the ZDNet Security newsletter now

Web performance company CloudFlare reported that it mitigated a Distributed Denial of Service (DDoS) attack on a French Website that reached a record-setting attack of almost 400 Gigabits per second (Gbps).

This wasn’t just boasting, Arbor Networks, a DDoS security company and CloudFlare rival, agreed that the attack reached at least 325Gbps.

London teen charged over Spamhaus mega-DDoS attacks

An unnamed London teenager has been charged with a series of criminal offenses following a series of denial-of-service attacks against internet exchanges and the Spamhaus anti-spam service last year. The 17-year-old male from London was charged on Friday and faces computer misuse, fraud and money-laundering offenses at a hearing ...

By John Leyden. 30 Jun 2014

Hong Kong as a Target of DDoS Attacks (September-October)

Number of Observed DDoS Attacks

The following graph illustrates that the number of observed DDoS attacks targeting Hong Kong-related online properties more than doubled between September and October, from 1,688 discrete attacks in September to 3,565 attacks in October.

24 million home routers expose ISPs to massive DNS-based DDoS attacks
Apr 2, 2014

Gaps in existing DDoS defenses require highly targeted DNS defenses to eliminate malicious traffic

World of Warcraft Expansion Hit with DDoS Attack
TAGS: Gaming, Security

London teen charged over Spamhaus mega-DDoS attacks
An unnamed London teenager has been charged with a series of criminal offenses following a series of denial-of-service attacks against internet exchanges and the Spamhaus anti-spam service last year. The 17-year-old male from London was charged on Friday and faces computer misuse, fraud and money-laundering offenses at a hearing ...

By John Leyden. 30 Jun 2014

Sony confirm DDOS attack after Lizard Squad claim PSN 'take down' affecting PS4 and PS3

SONY have confirmed the Playstation Network was hit by a DDOS attack this week, affecting both the PS4 and PS3.

World of Warcraft Expansion Hit with DDoS Attack
TAGS: Gaming, Security

London teen charged over Spamhaus mega-DDoS attacks
An unnamed London teenager has been charged with a series of criminal offenses following a series of denial-of-service attacks against internet exchanges and the Spamhaus anti-spam service last year. The 17-year-old male from London was charged on Friday and faces computer misuse, fraud and money-laundering offenses at a hearing ...

By John Leyden. 30 Jun 2014

Sony confirm DDOS attack after Lizard Squad claim PSN 'take down' affecting PS4 and PS3

SONY have confirmed the Playstation Network was hit by a DDOS attack this week, affecting both the PS4 and PS3.

World of Warcraft Expansion Hit with DDoS Attack
TAGS: Gaming, Security

London teen charged over Spamhaus mega-DDoS attacks
An unnamed London teenager has been charged with a series of criminal offenses following a series of denial-of-service attacks against internet exchanges and the Spamhaus anti-spam service last year. The 17-year-old male from London was charged on Friday and faces computer misuse, fraud and money-laundering offenses at a hearing ...

By John Leyden. 30 Jun 2014

Sony confirm DDOS attack after Lizard Squad claim PSN 'take down' affecting PS4 and PS3

SONY have confirmed the Playstation Network was hit by a DDOS attack this week, affecting both the PS4 and PS3.

World of Warcraft Expansion Hit with DDoS Attack
TAGS: Gaming, Security

London teen charged over Spamhaus mega-DDoS attacks
An unnamed London teenager has been charged with a series of criminal offenses following a series of denial-of-service attacks against internet exchanges and the Spamhaus anti-spam service last year. The 17-year-old male from London was charged on Friday and faces computer misuse, fraud and money-laundering offenses at a hearing ...

By John Leyden. 30 Jun 2014
Defining Distributed Denial of Service (DDoS)

- Denial of Service Attacks have different nature
  - Application-layer attacks
    - Handled by the Security Appliances and Endpoint Security
    - Mitigated by NGFW, NGIPS, AMP and other L7 security technologies
  - Volumetric DDoS attacks
    - Should be handled at the SP Edge or Core
    - Too late for mitigation on the Enterprise DC/DMZ side

- DDoS types based on the network traffic used
  - L3/L4 attacks
    - ICMP Flood, TCP SYN, UDP Frag
  - Distributed Reflection DoS (DrDoS) Amplification attacks
    - DNS, NTP, CharGen, SNMP
    - UDP-Based, Spoofed Source Address, Bandwidth Amplification Factor 500+ times
  - L7 attacks
    - HTTP GET/POST, SIP, SSL
DDoS Attacks Protection Options

- Depending on sophistication level of technology involved
  - **Blackholing** with Remote Triggered BlackHoling (RTBH)
    - BGP dummy route advertised
    - Route to `null0` or route to a forensic network analysis
    - RFC 3882, RFC 5635 (D/RTBH and S/RTBH)
    - **All traffic to victim discarded** (good and bad)
    - Damage Limited, but victim still unreachable
    - Granularity with BGP FlowSpec
      - Match L3/L4 Source, Destination, Port, Size, QoS Rate-Limit
      - RFC 5575 Dissemination of Flow Specification Rules
      - `draft-ietf-idr-flow-spec-v6-06`, initially `draft-raszuk-idr-flow-spec-v6-01`
  - **Sinkholing** with diversion to the scrubbing infrastructure
    - Centralized, Distributed, Mixed deployment models
    - Differentiating good and bad traffic
    - Only **bad traffic to victim discarded**
    - Damage avoided, if scrubbing successful
    - AntiDDoS is a **highly intelligent system** to handle elaborate attacks
Remotely Triggered Black Holes (RTBH)

- Route an IP address or prefix to the **bit bucket at the network edge**
  - Prevent malicious traffic from entering the secure network and consuming resources
  - **Destination blocking** temporarily drops all traffic to a protected resource until the attack stops
  - **Source blocking** drops all traffic from a malicious host or subnet at the perimeter

- Basic routing features **propagate a drop rule** across administrative domains
  - Ability to set an arbitrary next-hop in BGP, Null0 static routes, and Reverse Path Forwarding (RPF)
  - Trigger device injects the rule into iBGP routing domain, blocking router drops traffic based on rule

- ASA can operate as the trigger or blocking device with BGP starting **9.2(1)**
**RTBH Trigger on ASA Example**

1. Establish BGP peering between the ASA and perimeter router with RTBH configuration.

2. ASA administrator identifies 10.1.1.1 as a malicious host, configures a block rule.

3. Subsequent packets from 10.1.1.1 are dropped at the Provider Edge router.

   - **Create a route map to set the next hop for any matching advertised routes to the “blackhole” IP address**
   
   ```
   route-map RTBH
   set ip next-hop 192.0.2.1
   set origin igp
   set community no-export
   router bgp 65001
   neighbor 192.168.100.1 remote-as 65001
   redistribute static route-map RTBH
   
   route Null0 10.1.1.1 255.255.255.255
   ```

   - **Redistribute all static routes using the route map for blackholing**

   ```
   ip route 192.0.2.1 255.255.255.255 Null0
   ```

   - **Advertise a static route to the attacker using the route-map**

   ```
   redistribute static route-map RTBH
   ```

   - **“Soft” uRPF ensures that each source IP address has a valid return route**

   ```
   ip verify unicast source reachable-via any
   interface Null0
   no ip unreachables
   router bgp 65001
   neighbor 192.168.1.1 remote-as 65001
   ```

   - **Any traffic recursively routed to the blackhole IP address will be dropped**
DDoS Mitigation – BGP RTBH @Cisco

- OER – Optimized Edge Routing
- Also known as Performance Routing (PfR)
- Immediately install `null0` route
- Avoid costly ACL and FW rule change
- Used with iBGP and uRPF
- No additional config involved

- Configure a `/32 null0` route:

```plaintext
route x.x.x.x 255.255.255.255 null0
```
DDoS Mitigation with Scrubbing Infrastructure

- **Detection** action, identifying an abnormal behavior in the network and trigger an alert for the operator. Sends SNMP interface polling, IPFIX, sFlow, **Netflow v5/v9 (FNF)** to Collector

- **Diversion (offRamp)** action of diverting traffic targeted to the victim to the scrubbing device. **BGP FlowSpec**, Policy-Based Routing, Specific Route Injection

- **Mitigation** action performed by the cleaning device to differentiate legit traffic from attack traffic and block the attack. Scrubber Appliance or Router Module (ASR9k VSM)

- **Re-injection (onRamp)** action of re-injecting the legit traffic into the network and guarantee it will be able to reach the destination
DDoS Mitigation Scenarios

**SP Edge Deployment**
- Distributed Scrubbers
- Scrub traffic entering SP
- Serving Customers, DCs, SP

**SP Centralized Deployment**
- Local and Long Diversion (GRE)
- Centralize Scrubbing HW Resources
- Serving Customers, DCs, SP

**Enterprise Edge Deployment**
- At the Enterprise Peering Point
- Serving Enterprise Customer
- **Clean Pipe not achieved**

Can be Always-On with Permanent Redirections
Arbor Networks and Cisco Partnership

- **Peakflow SP** (known as Collector Platform CP)
  - Collects Flow records
  - Detects abnormal network behavior and triggers alerts
  - Can influence the routing, injecting BGP routes in the network
  - Supports **BGP FlowSpec** as a Controller
  - Sets up and monitors the TMS remotely

- **Peakflow SP Threat Management System (TMS)**
  - Configured by CP, receives diverted traffic and proceeds to in-depth packet analysis
  - Discards the attack packets and transmits the legit ones
  - Provides real-time monitoring info to operators
  - Standalone Appliance or hosted on Cisco ASR 9000 **VSM** module
Arbor TMS on ASR9k VSM

- **Virtualized Services Module (VSM)** with
  - All ASR 9000 chassis except 9001
  - RSP440 onwards (not RSP2)

- **Multi-Purpose Service Card**
  - 40 x86 CPU cores, 128GB RAM, 120Gbps backplane
  - CGN/CGv6, IPSec, Mobile GW, DPI, ASAv
  - **DDoS Mitigation, hosting ArbUX OS**
    - 40Gbps of scrubbing performance
  - Service chaining
  - KVM virtualized environment
  - OnePK API/SDK

- Less elaborate, stateless attacks can still be **stopped at the router level**, saving VSM CPU

Old-School Best Practices are valid today more than ever
  – Physical Infrastructure Integrity, can it be guaranteed?
  – Software Integrity, platform OS attacks demonstrated
  – Hardening the Control, Management and Data Planes

DDoS attacks are the primary threat at Internet Scale
  – Develop and deploy an antiDDoS strategy, talk to your SP
    ▪ SP- or Enterprise side
    ▪ Distributed or Centralized
    ▪ Blackholing, Sinkholing or Scrubbing
  – When the attack hits, it is already too late when unprepared

Be a good Internet Citizen
  – Don’t let the configuration error result in a massive Prefix Hijacking
  – Don’t let your Network originate DDoS Attacks!
Firewall Deployment and Segmentation
The Fatal Assumptions:

1. **High availability** is being used  
   – Failover, Etherchannel, Routing, VPN HA  
2. My network is **properly segmented**  
   – Employing Interface Security logic  
3. Firewall does its **stateful filtering job**  
   – Managing IPv4|v6 ACLs effectively  
4. I **understand my NAT|PAT statements**  
   – Config complexity rises over time
Firewall High Availability is used

- Assume ASA deployed in **routed single-context** mode Active-Standby Failover pair. Failover is the most mature HA technology today:
  - Stateful sub-second failover will be used
  - Failover and state interfaces, with IPSec encryption since 9.1(2)
- Link-level redundancy with **Etherchannel** (1G/10G)
  - Best redundancy in stacked/VSS/vPC topologies
  - Redundant interfaces approach may still be used
- ASA OSPF FastHello 9.2.(1), NSF Graceful Restart 9.3(1)
  - Set the OSPF dead interval above the failover unit polltime, otherwise the OSPF adjacency will expire before switchover happens
- Notable capabilities introduced in ASA 9.3(2)
  - **Interface Zones**, enables true multi-homing (think IOS ZBFW)
  - Up to 8 interfaces within a Traffic Zone
  - **Equal-Cost Multi-Path** (ECMP) routing
  - Allowing up to 8 static/dynamic routes per zone
The overall ASA **High Availability strategy** is:
- Bring Clustering feature support on par with Failover
- Retain it as the only HA mechanism long term
- No reason to have two HA features, Clustering is superior to Failover in every aspect

The answer to Clustering can be yes, if:
- Need **true Active/Active** HA with performance scaling and resiliency
- **Pure Firewalling** desired, NAT scale considerations
- Avoid **centralized** features like site-to-site VPN, multicast, many of the inspection engines
- Understand some features **unsupported**, like remote access VPNs, advanced MPF protocol inspections, WCCP, BTF and UC Security

BRKSEC-3032 Advanced ASA Clustering Deep Dive
May I use ASA for EBGP Peering? Yes, but no.

- **ASA 9.3(2)** supports BGPv4 and BGPv6 for dynamic routing across all platforms
  - Standard communities and all path attributes, route redistribution
  - Confederations, route reflectors, tagging, neighbor source-interface, and BFD are **not supported**
  - BGP RIB is replicated in failover along with other protocols
  - Single and multiple-context modes with a single Autonomous System
  - No hard prefix limit, but tested officially up to 100K prefixes, 500 neighbors on ASA 5585-X SSP60

```
! System Context
router bgp 65001
  bgp fast-external-fallover
! Context A
router bgp 65001
  address-family ipv4 unicast
  neighbor 192.168.1.101 remote-as 65002
! Context B
router bgp 65001
  address-family ipv4 unicast
  neighbor 192.168.2.200 remote-as 65003
```

- Global BGP parameters are controlled from the system context
- Neighbors are configured in the application contexts
- AS number in all application contexts must match the system context
ASA BGP Use Cases

- Software release 9.2(1)
- Transit BGP-aware firewall with a single routing path, parity to existing DRP
- No same-prefix routes across different logical interfaces
- Same-prefix load-balancing across up to 3 next hops on same logical interface

- Use EtherChannel with vPC/VSS for Layer 2 interface redundancy
- Layer 3 redundancy is achieved with multiple next hops on the same logical interface

- Software release 9.3(2)
- Same-prefix load-balancing across multiple logical interfaces may cause state asymmetry along the reverse path
- Support requires more than just simple load-balancing at Layer 3

- Use EtherChannel with vPC/VSS for Layer 2 interface redundancy
- Layer 3 redundancy is achieved with multiple next hops on the same logical interface
ASA Multihoming with Interface Security Zones

- ASA routing table was based on logical (named) interfaces till 9.3(1)
  - Each IP prefix can be routed to one logical interface at any given time
  - Equal Cost Multi Path (ECMP) support with up to 3 next hops on one logical interface
  - Asymmetrical routing requires open ACLs and TCP State Bypass
  - ASR Groups may help in Active/Active failover, but require redirection

- Assign multiple logical interfaces to a Security Zone ASA 9.3(2)
  - Same-prefix ECMP with up to 8 next hops across all interfaces in a zone
  - Return traffic matched to the connection entry from any interface in a zone
  - Seamless connection switchover to another egress interface in the same zone on failure
  - No support for unequal cost load-balancing with EIGRP variance today
Configuring ASA Security Zones

- Zones are only supported in **routed firewall** mode, starting 9.3(2) software release
  - Each interface belongs to its own implicit zone by default
  - **Security levels must match** across all interfaces in a zone
  - ASR Groups cannot be configured in the same context as zones

```
zone outside-zone
  interface GigabitEthernet0/0
  nameif outside1
  zone-member outside-zone
  ip address 192.168.1.1 255.255.255.0

interface GigabitEthernet0/1
  nameif outside2
  zone-member outside-zone
  ip address 172.16.171.1 255.255.255.0
```

- Connection entry is tied to the original (**primary**) interface for its lifetime
  - **Current** egress interface may differ from the primary interface after a path switchover

```
asa# show conn detail
TCP outside-zone:outside1(outside2): 10.1.1.1/80 (10.1.1.1/80) inside-zone:inside1(inside1):
10.2.2.2/34254 (10.2.2.2/34254), flags UO, idle 12s, uptime 13s, timeout 1h0m, bytes 16
```

- Connection is always cleared if the primary interface is removed from the zone or unconfigured
ASA Security Zone Interface Equivalency

- Config must ensure fully homogenic ACL and NAT configuration across all zone members:

  - Available 9.3(2). Zone-level configuration model will be provided in a later release
  - Member interfaces with different mapped NAT spaces do not support existing connection switchover

- Identical static or dynamic ECMP routes must be present across all zone members:

  - ASA will attempt a route lookup outside of the zone if no successor route exists across zone members
  - Route lookup always prefers the original interface, if still available

```plaintext
object network INSIDE_HOST
  host 192.168.0.100
  nat (inside,any) static 10.1.1.10
  access-group INBOUND in interface outside1
  access-group INBOUND in interface outside2

route outside1 0.0.0.0 0.0.0.0 192.168.1.100
route outside2 0.0.0.0 0.0.0.0 172.16.171.100
```

- Use any mapped interface or separate NAT rules
- Apply same interface ACL to all zone members or use global ACL
ASA Interface Security Levels (0-100)
- Fundamental logical segmentation construct
- Applied to ASA physical and subinterfaces
- Will be mapped later to NGFW/NGIPS zones
- Inside is trusted with security-level 100
- Outside is untrusted with security-level 0
- Balance between complexity and secure isolation
- Create Multiple DMZs with security-level <1-99>
- Organize and isolate servers into groups to limit lateral movement in case of breach

ASA Security-level logic:
- From higher to lower security permitted by default
- From lower to higher security interface requires ACL
- By default, no nat-control enables traffic flow without NAT/PAT statements
My Firewall does its stateful filtering job

- ASA is a purpose-built appliance to **handle large ACLs**
  - ASA5585-X SSP60 can scale up to 2M+ ACEs
  - Extended and Global Unified ACLs with objects used for Firewall rules
  - ACLs reference real IP addresses in the rules

- **Long-term strategy to maintain ACLs:**
  - ACL remarks help to understand what was configured
  - Objects and ASDM/CSM GUI can enhance operations
  - Packet Tracer utility proves extremely useful

- **Extended ACLs go beyond** traditional IP, Ports and ICMP:
  - User and Group (IDFW with CDA and Active Directory) 8.4(2)
  - DNS FQDN 8.4(2) objects
  - TrustSec SGACL with SXP 9.0(1), inline transport 9.3(1)
  - Mixing object types in one ACE is a powerful capability

- ASA 9.3(2) introduces **ACL Config Session** concept:
  - Transactional commit 9.1(5)
  - Free changes during the config session
  - Forward-reference enables used objects modification

---

User and Group with Identity Object Group IDFW Global ACL

```plaintext
object-group user asausers
  user CISCO\gmikolaj
  user-group CISCO\group.chambers
access-list IDFW_ACL extended permit ip object-group-user asausers any any
access-group IDFW_ACL global
```

FQDN-based extended interface ACL

```plaintext
object network sarmatia
  fqdn warsaw.emea.cisco.com
object network google
  fqdn www.google.com
object-group network search-engine-group
  network-object google
access-list FQDN_ACL extended permit tcp object sarmatia object-group search-engine-group eq 443
access-group FQDN_ACL in interface dmz44
```

SGT-based TrustSec SGACL

```plaintext
object-group security objgrp-sg-hr-mgrs
  security-group tag 1
object-group security objgrp-sg-hr-network
  security-group tag 2
access-list HR_ACL permit ip object-group-security objgrp-sg-hr-mgrs any any
access-group HR_ACL in interface dmz44
```

---

Presentation_ID Cisco and/or its affiliates. All rights reserved.
Stateful Firewall Best Practices

- The firewall can be a chokepoint if not properly sized.
  - Firewall is **not a replacement** for an antiDDoS solution.

- Understand your ACLs:
  - Document firewall rules
  - Perform regular **rule audits**
  - **Zero hit count** rules
    - Why are they here?
    - Harder to migrate to new hardware, carrying thousands of legacy rules
    - Potential to leave holes in the future, scared to delete rules
  - Inside to outside policies more open than need to be
    - Dead ports/protocols, or no business use
  - **Rules in wrong place**
    - Take advantage of the router stateless ACLs at the Edge
    - Filter coarse to fine, moving from outside to inside
  - Segmentation is being improperly done
    - Opening all standard ports make controls ineffective
  - Use management tools properly to **handle the ACL at scale**
ASA Access Lists Scale

- Recommended maximum ACEs to limit connection setup rate impact (<10%)
- Higher scale achieved with **64-bit 8.4+** software on ASA5585-X

<table>
<thead>
<tr>
<th>ASA Hardware Platform</th>
<th>5580-20</th>
<th>5580-40</th>
<th>5585-10</th>
<th>5585-20</th>
<th>5585-40</th>
<th>5585-60</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(&lt;8.3, 32-bit)</td>
<td>750K</td>
<td>750K</td>
<td>500K</td>
<td>750K</td>
<td>750K</td>
<td>750K</td>
</tr>
<tr>
<td>Maximum recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(8.4, 64-bit)</td>
<td>1M</td>
<td>2M</td>
<td>500K</td>
<td>750K</td>
<td>1M</td>
<td>2M</td>
</tr>
</tbody>
</table>

- **ASA5500-X and ASASM run only 64-bit software**

<table>
<thead>
<tr>
<th>ASA Hardware Platform</th>
<th>5512-X</th>
<th>5515-X</th>
<th>5525-X</th>
<th>5545-X</th>
<th>5555-X</th>
<th>ASASM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum recommended</td>
<td>100K</td>
<td>100K</td>
<td>250K</td>
<td>400K</td>
<td>600K</td>
<td>2M</td>
</tr>
</tbody>
</table>
ASA nat-control mechanism disabled by default
- Fundamental to understanding NAT operations
- Considered deprecated today
- If enabled, a translation is required for a connection creation
- Packet not matching any NAT statement is dropped

NAT processing order is top-down, like ACLs (Rule ID)
- Manual NAT (Twice NAT) evaluated first, the order matters
  - Source and destination NAT in a single line
  - Bi-directional translations
  - One-to-one, one-to-many, many-to-many and many-to-one
- Automatic NAT (Auto NAT or Object-based) processed next
  - Single rule per object, when Manual NAT not needed
- Auto NAT order of precedence:
  - Static Rules preferred over Dynamic Rules
  - Smaller Objects (Hosts) preferred over Larger (Subnet)
  - Lower Numeric IP Prefix (starting from first IP address octet)
  - Lowest Alphanumeric Object Name
- After-Auto Twice NAT evaluated last
  - Avoid where possible

---

object network myInsideNetwork
  subnet 10.1.2.0 255.255.255.0
object network DMZnetwork1
  subnet 209.165.201.0 255.255.255.224
object network PATaddress1
  host 209.165.202.129

nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1

object network STATIC_MAPPING
  range 198.51.100.50 198.51.100.60
object network INSIDE_SERVERS
  range 192.168.1.35 192.168.1.45
nat (inside,outside) static STATIC_MAPPING

object network INSIDE_WEB_SERVER
  host 192.168.1.55
nat (inside,outside) static 198.51.100.75 service tcp 80 8080

object network INSIDE_NETWORK
  subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic NAT_POOL interface
ASA Software 9.3
New Features and Enhancements

40+ new features in 9.3(1) and 9.3(2) software releases.

Most notably for Internet Edge Use Cases:

- **Configuration Session** with ACL Transactional Commit and Forward-Reference
- Interface **Traffic Zones**, route redundancy and asymmetric routing
- Equal-Cost Multi-Path (**ECMP**) up to 8 next-hops across interfaces in a zone
- BGP and OSPF **Non-Stop Forwarding** (**NSF**) (NSF)
- Transparent mode Bridge-Group increase from 8 to 250 bridge-groups per context
- **ASA Image Signing and Verification**
- TrustSec L2 inline SGT Support
- **ASA RESTful API** 1.0 for configuration and management
"NAT64 IP\[n] = \sqrt{\sum_{i=1}^{\infty} evil}

"
Elevating Visibility and Control with NGFW
Internet Edge – Next-Generation Firewalls

The Fatal Assumptions:

1. I am **controlling the right traffic**
   - NGFW network placement and redirection

2. My **NGFW** is more than a toy
   - Using Application Risks and Relevance

3. **Context** means more than marketing
   - User Awareness and Identity

4. I am **limiting the attack surface**
   - Applying NGFW access policies

BRKSEC-2028 Deploying Next-Generation Firewall with ASA and FirePOWER Services
I am controlling the right traffic with NGFW

- Traffic Redirection to NGFW HW/SW Module achieved with ASA MPF Service Policies
- Can be matched based on interface, source / destination, protocol ports and ASA user identity
- In Multi-context Mode, different ASA FirePOWER policies can be assigned to each context
- **Fail-open** and **Fail-closed** failure scenarios
- Passive **monitor-only**, copy of the traffic sent to module. Applicable for demo or IDS-mode deployment with NGIPS feature-set.
- Redirect all the traffic for inline NGFW:

  ```
  policy-map global_policy
  class class-default
  sfr fail-open
  service-policy global_policy global
  ```
ASA FirePOWER Functional Distribution

URL Category/Reputation
NGIPS
Application Visibility and Control
File Type Filtering
Advanced Malware Protection
File Capture
TCP Normalization
NAT
TCP Intercept
Routing
IP Option Inspection
ACL
IP Fragmentation
VPN Termination
Botnet Traffic Filter

FirePOWER NGFW Module
ASA Firewall

Cisco ASDM-IDM Launcher
Cisco Security Manager
My NGFW is more than a toy

- Examining the Host Discovery process with Context Explorer: **OS and Traffic by IP and User**

- Understanding host traffic by **Risk, Intrusion Events, Business Relevance and Web Application**
NGFW Application Risks and Relevance

• Understanding the **Application environment** in the FireSIGHT Application Dashboard

  - Traffic by Application
  - Allowed Connections by Application
  - Denied Connections by Application
  - Unique Applications over Time

• Evaluating the Applications by Risk and Business Relevance at the Internet Edge

  - **Application risk** – likelihood that an application’s use may violate your organization’s security policy. Can range from very low to very high.
    - Peer-to-peer applications tend to have a very high risk.

  - **Business relevance** – likelihood that an application is used within the context of your organization’s business operations, as opposed to recreationally. Can range from very low to very high.
    - Gaming applications tend to have a very low business relevance.
Context-Awareness means more than Marketing

- Viewing User Login Activity
- Examining the User Statistics Dashboard

- We will discuss the importance of Context in greater detail later in this session

- Unique Users over Time
- Traffic by Initiator User
- Allowed Connections by User
- Denied Connections by User
I am limiting the Attack surface with Access Policies

### Block High Risk Application Protocols from User Groups

<table>
<thead>
<tr>
<th>Block</th>
<th>Risk</th>
<th>Protocol Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Block VPN/Tunnel, Anonymizer Application Protocols from User Groups

<table>
<thead>
<tr>
<th>Block</th>
<th>Security Risk</th>
<th>Protocol Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td>VPN/tunnel, anonymizer,</td>
</tr>
</tbody>
</table>

### Allow Remote Administration Application Protocols to DMZ-Hosted Services

<table>
<thead>
<tr>
<th>Allow</th>
<th>Protocol Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted Services</td>
<td>VPN/tunnel, remote administration, web services provider</td>
</tr>
</tbody>
</table>

### Interactive Block Specific Application Protocols to Finance Application DMZ

<table>
<thead>
<tr>
<th>Block</th>
<th>Risk</th>
<th>Protocol Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td>SMS tools, VPN/tunnel,</td>
</tr>
</tbody>
</table>

### Allow Low Risk Applications from Users to the Internet

<table>
<thead>
<tr>
<th>Allow</th>
<th>Risk</th>
<th>Protocol Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td>Facebook post, Gnutella,</td>
</tr>
</tbody>
</table>
Internet Edge NGFW – Summary

Picking The Right Technology

- Require integrated NGFW and robust network firewall at the Internet Edge with performance up to 15Gbps inspected traffic:
  - **ASA FirePOWER Services** with 5500-X, 5585-X appliance family is the best fit
  - All the ASA features up to 9.3(2) software supported, robust network FW capabilities
  - Single and multi-context, routed and transparent modes
  - Can act as an integrated IPSec VPN headend in smaller deployments
  - All the 5.4 FirePOWER NGFW software features minus SSL decryption

- Require standalone purpose-built NGFW appliance with performance up to 60Gbps inspected traffic:
  - **FirePOWER Appliances** inline behind Internet Edge Network Firewall
  - Wide variety of form-factors and interface densities, performance from 50Mbps to 60Gbps
  - All the 5.4 FirePOWER software features including SSL decryption

- **FireSIGHT Management Center** is a mandatory component for both the above.
Finding Needles in the Haystack with NGIPS Threat Prevention
Internet Edge Next-Generation Intrusion Prevention

The Fatal Assumptions:

1. I know my threat landscape
   – Host Discovery process

2. I am protected from relevant threats
   – Tuning NGIPS for the threat coverage

3. I can focus on the important stuff
   – Utilizing the Impact Levels

4. When breach occurs, I know it
   – Indicators of Compromise (IoC)
NGIPS with FireSIGHT Management Center constantly builds the knowledge database by passive network discovery, populating the Host Profiles.

Host profile information includes:
- IP Address, MAC, Hostname, NetBIOS name
- Device (Hops), Host Type, Last Seen
- Current User, User History
- Operating System Vendor/Product/Version
- Client Protocol, Version, Application
- Server Vendor, Version, Protocol, Port, Application
- Web Applications, Version, Content
- White List Violations, Type, Reason, White List
- Malware Detections, Time, Threat, File Name, File Type
- Mapped Vulnerabilities, Name, Remote, Port
Working with Host Profiles (1/3)

Understanding the **Host OS summary** and **Hosts Table**, utilizing elastic search.

<table>
<thead>
<tr>
<th>OS Vendor</th>
<th>OS Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Windows</td>
<td>3,625</td>
</tr>
<tr>
<td>pending</td>
<td>pending</td>
<td>1,046</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>Linux</td>
<td>1,568</td>
</tr>
<tr>
<td>Apple</td>
<td>Mac OS</td>
<td>596</td>
</tr>
<tr>
<td>Linux</td>
<td>Linux</td>
<td>333</td>
</tr>
<tr>
<td>GentOS</td>
<td>Linux</td>
<td>214</td>
</tr>
<tr>
<td>Google</td>
<td>Android</td>
<td>212</td>
</tr>
<tr>
<td>Google</td>
<td>Chromium</td>
<td>122</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Phone</td>
<td>105</td>
</tr>
<tr>
<td>IBM</td>
<td>AIX</td>
<td>79</td>
</tr>
<tr>
<td>Firefox</td>
<td>Firefox</td>
<td>23</td>
</tr>
<tr>
<td>Apple</td>
<td>iOS</td>
<td>13</td>
</tr>
<tr>
<td>VMware</td>
<td>ESXi</td>
<td>11</td>
</tr>
<tr>
<td>VMware</td>
<td>ESX</td>
<td>10</td>
</tr>
<tr>
<td>Red Hat</td>
<td>Enterprise Linux</td>
<td>9</td>
</tr>
<tr>
<td>OpenBSD</td>
<td>User</td>
<td>6</td>
</tr>
<tr>
<td>SuSE</td>
<td>SUSE</td>
<td>3</td>
</tr>
<tr>
<td>OpenBSD</td>
<td>User</td>
<td>3</td>
</tr>
<tr>
<td>Mandriva</td>
<td>Linux</td>
<td>2</td>
</tr>
<tr>
<td>Slackware</td>
<td>Linux</td>
<td>2</td>
</tr>
<tr>
<td>Solaris</td>
<td>Linux</td>
<td>1</td>
</tr>
<tr>
<td>Etherbox/Sun</td>
<td>Solaris</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Current User</th>
<th>Host Type</th>
<th>OS Vendor</th>
<th>OS Name</th>
<th>OS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.30.124</td>
<td>Deanna Meyer (dmeyer, LDAP)</td>
<td>Host</td>
<td>Ubuntu</td>
<td>Linux</td>
<td>10.10</td>
</tr>
<tr>
<td>10.0.30.129</td>
<td>Douglas Gronick (dgronick, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>7, Server 2008 R2</td>
</tr>
<tr>
<td>10.0.30.130</td>
<td>Josh Harrill (jharrill, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.130</td>
<td>Clair Hecto (chector, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.130</td>
<td>Jan Mikovsky (jmikovsky, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>7, Server 2008 R2</td>
</tr>
<tr>
<td>10.0.30.133</td>
<td>Ted Bromer (tbroner, LDAP)</td>
<td>Host</td>
<td>Ubuntu</td>
<td>Linux</td>
<td>13.10</td>
</tr>
<tr>
<td>10.0.30.134</td>
<td>Katrina Flood (kflood, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.135</td>
<td>Jan B. Pak (jpak, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.136</td>
<td>Michael Holm (molhm, LDAP)</td>
<td>Host</td>
<td>Ubuntu</td>
<td>Linux</td>
<td>13.10</td>
</tr>
<tr>
<td>10.0.30.137</td>
<td>Patricia Doyle (pdoyle, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>8</td>
</tr>
<tr>
<td>10.0.30.139</td>
<td>David Simpson (dsimpson, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.141</td>
<td>Jon Morris (jmorris, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.141</td>
<td>Steve Nagata (snagata, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.142</td>
<td>Pat Coleman (pcoleman, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.144</td>
<td>Jon Morris (jmorris, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
<tr>
<td>10.0.30.147</td>
<td>Andrew Dixon (adixon, LDAP)</td>
<td>Host</td>
<td>Microsoft</td>
<td>Windows</td>
<td>2000, XP, Server 2003</td>
</tr>
</tbody>
</table>
Working with Host Profiles (2/3)
Analyzing the specific machine Host Profile

- **Basic Host Information**: IP Address, NetBIOS Name, Hops from NGIPS, MAC Address, Host Type, Last Seen, Current User

- **Indicators of Compromise (IoC)**

- **Detected Operating System (OS)**

- **Detected Servers** Running on Host

- **Detected Applications**

- **Last 24 hours of User Activity**
Working with Host Profiles (3/3)

Analyzing specific machine Host Profile (continued)

- **Host Attributes. Criticality**
  - used in Correlation Policies

**Discovered Protocols**

**White List Violations.** Special kind of correlation event, indicating violation of operating systems, application protocols, clients, web applications, and protocols that are allowed to run on a specific subnet.

**Vulnerabilities** section lists vulnerabilities based on the operating system, servers, and applications that the system detected on the host.

- If you import vulnerabilities from a QualysGuard Scanner, host profiles will include a QualysGuard Vulnerabilities section.
I am protected from relevant threats

FireSIGHT Recommendations in Intrusion Policies

Powerful capability that **recommends** which NGIPS rules should be **enabled or disabled** in your intrusion policy, **based on information** from the Network Map.

- You can choose to allow the system to modify rule states based on recommendations. The system adds a read-only **FireSIGHT Recommendations layer**.
Advanced FireSIGHT Recommendations Settings

- Configure the FireSIGHT Recommended Rules feature by identifying networks to examine in the network map.

- NGIPS rates the overhead of each rule as none, low, medium, high, or very high, based on the potential impact on performance and the likelihood to generate false positives.

- Investigating rules that will be changed after applying the FireSIGHT Recommendations.

- Applying or updating the Recommendations. This can be automated.
Focus on the important stuff with Impact Flags

- For each NGIPS event, FireSIGHT adds an impact level icon: 1 for Act Immediately, Vulnerable; 2 for Investigate, Potentially Vulnerable; 3 for Good to Know, Currently Not Vulnerable; 4 for Good to Know, Unknown Target; 0 for Good to Know, Unknown Network.

- Color indicates correlation between NGIPS data, network discovery, and vulnerability info.

- Investigate NGIPS Intrusion Events in FireSIGHT Security Analysis Dashboard.

<table>
<thead>
<tr>
<th>IMPACT FLAG</th>
<th>ADMINISTRATOR ACTION</th>
<th>WHY?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Act Immediately, Vulnerable</td>
<td>Event corresponds to vulnerability mapped to host</td>
</tr>
<tr>
<td>2</td>
<td>Investigate, Potentially Vulnerable</td>
<td>Relevant port open or protocol in use, but no vuln mapped</td>
</tr>
<tr>
<td>3</td>
<td>Good to Know, Currently Not Vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>4</td>
<td>Good to Know, Unknown Target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>0</td>
<td>Good to Know, Unknown Network</td>
<td>Unmonitored network</td>
</tr>
</tbody>
</table>
Investigate Important Intrusion Events

- Drilling into **Impact 1 Events** by User and Application

- Examining **Intrusions Not Dropped** and Top Targets
When Breach Occurs, I know it

NGIPS System correlates various types of event data to determine whether a host on monitored network is likely to be compromised:

- Intrusion events
- Security Intelligence
- Connection events
- File events
- Malware events

Hosts with active IoC tags appear in the IP Address columns of event views with a compromised host icon instead of the normal host icon.

A host can trigger multiple IoC tags. You can mark a host IOC as resolved, which removes that IOC tag from the host.

The Indications of Compromise section of the host profile displays all IoC tags for a host.

Indicator of Compromise (IoC) "in computer forensics is an artifact observed on a network or in operating system that with high confidence indicates a computer intrusion" [https://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/]
Working with IoCs in FireSIGHT – CnC Example (1/2)

- Highly Compromised Network with Multiple IoCs visible in Context Explorer

![Diagram showing IoC summary table view in Hosts Menu]

- IoC Summary Table View in Hosts Menu

- Drilling into and Examining CnC Security Intelligence IoC Events

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Detected</td>
<td>304</td>
</tr>
<tr>
<td>Impact 2 Attack</td>
<td>51</td>
</tr>
<tr>
<td>CnC Connected</td>
<td>53</td>
</tr>
<tr>
<td>Java Compromise</td>
<td>20</td>
</tr>
<tr>
<td>QuickTime Comromise</td>
<td>19</td>
</tr>
<tr>
<td>PowerPoint Compromise</td>
<td>14</td>
</tr>
<tr>
<td>Word Compromise</td>
<td>12</td>
</tr>
<tr>
<td>Adobe Reader Compromise</td>
<td>11</td>
</tr>
<tr>
<td>Excel Compromise</td>
<td>9</td>
</tr>
<tr>
<td>Impact 1 Attack</td>
<td>8</td>
</tr>
<tr>
<td>Dropper Infection</td>
<td>7</td>
</tr>
</tbody>
</table>

- IoC Events:
  - 172.16.0.75 (CnC Connected) Security Intelligence Event - CnC: The host may be under remote control (2015-01-04 19:18:00 - 2015-01-04 20:44:33)
Working with IoCs in FireSIGHT – CnC Example (2/2)

• Examining the Suspicious Host Profile
  
  ![Host Profile Image]
  
  **Indications of Compromise (1)**
  
<table>
<thead>
<tr>
<th>Category</th>
<th>Event Type</th>
<th>Description</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>CnC Connected</td>
<td>Security Intelligence Event</td>
<td>The host may be under remote control</td>
<td>2015-01-04 19:49:07</td>
<td>2015-01-04 20:33:30</td>
</tr>
</tbody>
</table>

• Investigating First Seen CnC Connection

• Next, employ the **AMP Network, Host Trajectories** and **NetFlow Forensics Analysis Data (CTD Solution)** for malware events and flows from this specific User/Host
Achieving High Security with NGIPS

- NGIPS is a **highly stateful** device
  - CPU-intensive nature of IPS it can create a DoS vector if positioned poorly
  - Performance considerations – need to choose hardware platform appropriately
  - Marketing vs **Real-life Performance** with Full Threat Coverage

- **NGIPS Placement:**
  - Putting outside of the firewall will produce noise instead of actionable events
  - Traffic flows understood, **Critical Assets** identified and protected

- **Common NGIPS Operations Challenges:**
  - Few organizations have **24x7 NOC/SOC** with eyes on monitoring tools
  - Few organizations tune policies, resulting in lots of noise
  - Few organizations staffed to **handle events**, monitoring might be good to outsource
  - **Living with the noise** and using IPS reactively, Post Mortem

---

**BRKSEC-3126** Advanced Configuration and Tuning of FirePOWER Services for ASA Modules and FirePOWER Appliances
FireSIGHT 3rd Party Integration through APIs

FireSIGHT Management Center is an open, API-driven System

1. Host Input API
   - **Enhance information** in the Network Map
   - Import data from 3rd party sources

2. eStreamer (Event Streamer) API
   - **Stream** several kinds of **event data** to a custom-developed client application. SIEM Integration

3. Remediation API
   - **Remediations launch** when conditions violate a correlation policy or compliance white list
   - **Automatically mitigate attacks** when you are not immediately available to address them
   - Ensure that system **remains compliant** with organization's security policy

4. External Database Access
   - **Query database** tables with a JDBC SSL client
   - Use an industry-standard **reporting tool**
   - Own **custom application** to query DB data

![Diagram of FireSIGHT integration with various tools and APIs](image-url)
FirePOWER | FireSIGHT Software 5.4
New NGFW and NGIPS Features and Enhancements

- **Inspecting the Uninspected**
  - Integrated **SSL Decryption** on Standalone FirePOWER Appliances
  - File-type Pre-Processor
  - Adobe SWF/Flash PDF Decompression Support

- **Simplified and Improved Detection**
  - **Unicode** filename support
  - Geolocation and Security Intelligence in Correlation Rules
  - **Protected Rule** Content

- **Platform Flexibility and Bandwidth**
  - **LACP** Link Aggregation
  - Vmware Tools FireSIGHT Support
  - **10Gbps Virtual Interfaces**
  - Multiple Management Interfaces
Next-Generation Intrusion Prevention @Cisco

- **350+** Cisco IPS sensors deployed today (4200 family)
- **1.5M** alerts / day
- **Migration** in progress, driven by:
  - FirePOWER Appliances
  - Network AMP Everywhere
  - TALOS Threat Intelligence
  - Contextual Analysis
  - Throughput and Capacity
  - API Integration
Internet Edge NGIPS – Summary
Picking The Right Technology

- Require integrated NGIPS and Network Firewall at the Internet Edge with performance up to 10Gbps inspected traffic:
  - **ASA FirePOWER Services** with 5500-X, 5585-X appliance family is the best fit
  - All the ASA features up to 9.3(2) software supported, robust FW capabilities
  - Single and multi-context, routed and transparent modes
  - Can act as an integrated IPSec VPN headend in smaller deployments
  - All the 5.4 FirePOWER software features minus SSL decryption

- Require standalone purpose-built NGIPS appliance with performance up to 60Gbps inspected traffic:
  - **FirePOWER Appliances** behind Network Firewall and Promiscuous SPAN deployments
  - Wide variety of form-factors and interface densities, performance from 50Mbps to 60Gbps
  - All the 5.4 FirePOWER software features including SSL decryption

- **FireSIGHT Management Center** is a mandatory component for both the above.
Web Security and Content Filtering
“Most organizations, large and small, have already been compromised and don’t even know it: 100 percent of business networks analyzed by Cisco have traffic going to websites that host malware.”

Cisco 2014 Annual Security Report
# Content Filtering – Web Security Options

<table>
<thead>
<tr>
<th>Solution</th>
<th>FirePOWER Services</th>
<th>Web Security Appliance (WSA)</th>
<th>Cloud Web Security (CWS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>ASA, FirePOWER Appliances</td>
<td>Physical and Virtual Appliances</td>
<td>Tower Redirection</td>
</tr>
<tr>
<td>Deployment</td>
<td>Physical Inline Deployment</td>
<td>Explicit and Transparent</td>
<td>On-Premise and Mobile</td>
</tr>
<tr>
<td>Use Case</td>
<td>NGFW Use Cases</td>
<td>Secure Web Proxy Use Cases</td>
<td>Cloud Proxy Use Cases</td>
</tr>
<tr>
<td>Integration</td>
<td>Internet Edge Placement</td>
<td>ASA and Switch with WCCPv2</td>
<td>ASA, WSA, ISR-G2, AnyConnect</td>
</tr>
<tr>
<td>Security</td>
<td>Reputation, NGIPS and AMP</td>
<td>Secure Web Proxy Use Cases</td>
<td>WBRS, OF, AV and AMP</td>
</tr>
<tr>
<td>SSL</td>
<td>Standalone SSL Decryption*</td>
<td>HTTPS Decryption</td>
<td>HTTPS Decryption</td>
</tr>
<tr>
<td>Identity</td>
<td>SFUA TUI</td>
<td>Use Cases</td>
<td>AAA, Cookie, EasyID AD, SAML</td>
</tr>
</tbody>
</table>

* SFUA TUI
Internet Edge Web Security

The Fatal Assumptions:

1. I have an **Internet Access Policy** in place
   - Users are aware and acknowledge it

2. All **users** are granularly **identified**
   - Utilizing context-awareness

3. I am **protected** from the **threats**
   - Multiple layers of defense

4. Guests are enforced with AUP
   - WLAN Anchor DMZ design with web filtering
Web Content Filtering Options: NGFW

- **ASA FirePOWER Services NGFW**
  - ASA 5500-X (SW) and 5585-X (HW module)
  - ASA integrated already at the Internet Edge
  - Traffic must be routed through NGFW
    - Alternatively, ASA acts as a VPN Headend
  - Additional functionality in existing NGFW deployment
  - URL Filtering in Access Policies
    - Categorization and Black/whitelisting
    - URL Reputation
  - Application Visibility (NAVL Engine)
    - Granular App visibility beyond HTTP/HTTPS
  - Geolocation Conditions (GeoDB)
  - Passive Identity with SFUA AD Connector
  - SSL inspection unavailable on-box ASA today
  - Requires FireSIGHT Management Center
I have an Internet Access Policy in place
Are Users aware of it?

• **Application Control** by:
  – Risks
  – Business Relevance,
  – Type
  – Categories
  – Tags
  – User-Created Filters

• **URL Control** by:
  – Categories (80+)
  – Reputation
  – Manual URL Objects
Content Filtering with FirePOWER (1/2)

Log **High Risk URLs** for InfoSec Purposes

Log **High Risk Applications** for InfoSec Purposes

Block **Non-Work Related** Content

Block **Banned Users**
### Content Filtering with FirePOWER (2/2)

#### Block Banned Applications

<table>
<thead>
<tr>
<th>Banned Apps</th>
<th>Finance</th>
<th>Operations</th>
<th>Social Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>BitTorrent</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>BitTorrent Sync</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>BitTorrent tracker</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>ExtraTorrent (2 more...)</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

#### Control Provocative URL Categories

<table>
<thead>
<tr>
<th>Provocative URL Categories</th>
<th>Finance</th>
<th>Operations</th>
<th>Social Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult and Pornography (Any Reputation)</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>Hate and Racism (Any Reputation)</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>Nudity (Any Reputation)</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>Pay to Surf (Any Reputation)</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

#### Block Finance from High Risk

<table>
<thead>
<tr>
<th>Finance from High Risk</th>
<th>Finance</th>
<th>Operations</th>
<th>Social Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

#### Block Operations from Social Networks

<table>
<thead>
<tr>
<th>Ops to SNS</th>
<th>Finance</th>
<th>Operations</th>
<th>Social Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>
Web Content Filtering Options: Web Proxy

- **Web Security Appliance (WSA)**
  - Purpose-Built AsyncOS Physical/Virtual Appliance
  - Explicit or Transparent Mode, HA options
  - HTTP, HTTPS, SOCKS, FTP, FTP over HTTP
  - URL Category Filtering
  - Advanced Web Application Controls
  - Time, Bandwidth Quotas, Streaming Rate-Limiting
  - Web Reputation (WBRS)
  - Multiple Antivirus Engines on-box (AV)
  - Advanced Malware Protection (AMP)
  - External DLP Engine integration with ICAP
  - Passive Identity (TUI) with CDA AD Connector
  - SSO identity options (NTLM, Kerberos)
  - AnyConnect Secure Mobility Integration
  - HTTPS decryption available on-box
  - On-box GUI or SMA centralized management
Explicit Proxy Deployment with WSA

Explicit means Client needs have proxy provisioned:
- Browser proxy setting (IP/port)
- PAC File
  - Via AD and GPO
  - Script or Manual
  - DHCP option 252
  - WPAD server

Explicit Proxy Workflow:
1. Client browses for a website
2. Browser connects to the WSA
3. DNS Resolution is done by WSA
   - A or AAAA record returned (IPv4|v6)
4. Firewall permits WSA web traffic only
5. WSA connects to the requested website
Transparent Proxy Deployment with WSA

WCCPv2 between network device and proxy
- Can be L2 or L3 (GRE) based
- Hash (SW) or Mask (HW) based assignment
- Input (ingress) or output (egress) redirect
- Load-balancing and redundancy, service groups

Transparent Proxy Workflow:
1. DNS Resolution is done by the Client
   - A or AAAA record returned (IPv4|v6)
2. Client browses for a website
3. Browser tries to connect to the website
4. Network device redirects the traffic to the WSA using WCCP, WSA spoofs SYN/ACK back to Client
   - Network device can be a Router, Switch or Firewall
5. WSA proxies the request
6. WSA inspects the content and returns to the Client
Transparent Proxy Considerations

Things to keep in mind when deploying ASA with WSA:
- ASA allows redirect in only
- One WSA instance cannot serve both inside and DMZ
- Interface ACL checked before WCCP redirection
- Can use permit and deny statements in redirect ACL
- Redirect method is GRE-based

Therefore, in this session, we will use an aggregation L3 inside cat6k/sup2T switch assuming the WCCP role
- Ingress L2 with Mask – recommended (in HW)
- Ingress L3 GRE with Mask – recommended (in HW)

For even larger scale, use persistence-based hardware or virtual loadbalancers with WSA(v) farm.
Achieving High Security with WSA

Web Security Appliance offers an in-depth, multi-layered security

- **Web Reputation** Scoring (WBRS) is the foundational mechanism
- **Apply Web Usage Controls** (WUC)
  - URL Filtering with Categories (URL) and SafeSearch
  - Recommend to have Dynamic Content Analysis (DCA) enabled for best results.
- Leverage the **Layer 4 Traffic Monitor** (L4TM) for threat visibility
- Enforce AUP with granular **Application Visibility and Control** (AVC)
  - Microapplication Control, Bandwidth Controls and Time/Volume Quotas
- Make use of **HTTPS Decryption** Policies where appropriate
- Utilize Signature-based real-time **Malware Scanners** (AV/AM)
  - Sophos, McAfee, Webroot. Adaptive Scanning dynamically chooses the best engine
- Use **Advanced Malware Protection** (AMP)
  - File Reputation, Sandboxing and Retrospection

TECSEC-2909 Web Security Best Practices Techtorial
Web Security Appliance AsyncOS 8.5
New Features and Enhancements

- Advanced Malware Protection (AMP) – Phase II
  - Ability to sandbox PDF and Microsoft Office files
  - In addition to EXE files supported in the first AMP release

- High Availability with failover groups using CARP

- Time and Bandwidth Quotas
  - Based on amount of data (in bytes) and/or time
  - Applicable to HTTP, HTTPS and FTP traffic
  - Custom end user notifications (EUN) when quota is close / exceeded
  - Configured under Access Policies and Decryption Policies

- Virtual SMA (Security Management Appliance) on ESXi 5.0, 5.1, 5.5

- ISE Integration (Early preview)
Cloud Proxy Considerations: ASA

CWS ASA Connector On-premise (9.0 software):

- Available with ASA 5500, 5500-X, 5585-X
- Transparent Deployment at Internet Edge
- Single/Multiple Context ASA support
- HTTP and HTTPS traffic
- Local whitelisting of the traffic
  - Useful for OS, Software updates, AV/AS signatures
- Automated failover to secondary CWS tower
- No dedicated hardware or software installation
- No end user browser changes
- Transparent User Identity with CDA and IDFW
- AAA Rules User Identity
- ASA inserts CWS headers with username/groups
  - X-Scansafe headers stripped by the CWS tower
- Robust scale up to 7.5K users behind ASA

CWS ASA Connector Workflow

CWS ASA Connector On-premise (9.0 software):

1. Client begins to establish connection to webserver IP (145.84.173.37 tcp/80)
2. ASA intercepts conn and redirects it to CWS Tower using tcp/8080
3. Client sends HTTP GET request
4. ASA appends X-ScanSafe information to HTTP Request Header
5. Cisco Cloud Web Security filters request and requests content from webserver
6. Data returned to Cisco Cloud Web Security, scanned and returned to Inside user

Problem: Cannot send HTTP/HTTPS flow for inspection to both ASA FirePOWER module and CWS at the same time.

Solution: Configure ASA MPF Policy. Send HTTP/HTTPS to CWS and the rest of the traffic to FirePOWER Services module.

Cloud Proxy Considerations: WSA

WSA Connector on-premise (WSA 8.0 software):

- Available with physical and virtual appliances
- Local web caching and DLP integration
- Local Explicit or Transparent WSA deployment
- Local user auth using CDA TUI and other methods
- WSA config via GUI config wizard
- Automated failover to secondary CWS tower
- WSA inserts CWS headers with username/groups
  - X-Scansafe headers stripped by the CWS tower
- Fail-open / fail-close mechanism
- Robust scale with x80 series appliances

Internet Edge Web Security @Cisco

- **Enterprise rollout**: Started small, then up to large campus sites
  - 4-6 **S680 appliances** deployed at each Internet POP (each large campus has a POP)
- **Cisco IT** currently uses two of many included technologies:
  - Web Based Reputation Filters (**WBRS**)
  - Webroot and McAfee **Anti-Malware** scanning engines
- **Not using URL filtering**, Cisco’s policy is to trust employees
- **Transparent** deployment (**WCCPv2**) to a **load-balanced pool** of Cisco WSAs
  - WSAs assess requested website based on “reputation score”
  - Compromised or malicious objects (or entire websites) are blocked
  - If reputation is not clearly excellent or poor, anti-malware services scan file
- **No SSL decryption** currently done by WSAs
- In one month at the RTP (Raleigh, North Carolina) location alone:
  - **1 Billion** HTTP Transactions processed
  - **10 Million** Transactions blocked (1%)
WSA Internet Edge Deployment @Cisco

- Protecting entire Cisco Network including:
  - Desktop and Mobile
  - Remote Access VPN
  - Internal Labs
  - DMZ Labs
  - Data Centers

- Deployment mode:
  - WCCPv2 Redirection
  - Backbone DMZ Gateways
  - Redundant Pair per GW
  - Common web ports
  - Reputation Scoring (WBRS)
Web Security Appliance @Cisco

Cisco Web Traffic Stats:
- HTTP is 25% of traffic + SSL 6%
- 12.5 TB in/out per day
- 330-360M web visits/day
- 6-7M (2%) blocked

WSA Blocked Transactions:
- 6.5M+ Malware sites blocked/day
- 93.5% - Web Reputation
- 4.5% - URL Category
- 2% - Anti-Malware

Malware Blocked in One Day:
- 441K – Trojan Horse
- 61K - Other Malware
- 29K - Encrypted Files (monitored)
- 16.4K - Adware Messages
- 1K – Trojan Downloaders
- 55 - Phishing URLs
- 22 - Commercial System Monitors
- 5 - Worms
- 3 - Dialers

WSA Blocked Transactions:
- 6.5M+ Malware sites blocked/day
- 93.5% - Web Reputation
- 4.5% - URL Category
- 2% - Anti-Malware
“Scaling from 3000 to 30,000 users only requires changing an access list, enabling WCCP on the routers, and pointing the routers to the Cisco WSAs.”

Jeff Bollinger
Senior Information Security Investigator
CSIRT @Cisco
Internet Edge Web Security – Summary
Picking The Right Technology

Depending on your goal, some solutions are more applicable:

- Local workforce with interest in HTTP/HTTPS-centric control
  - Web Security Appliance for purpose built Web filtering and control

- Require integrated support for more than just HTTP/HTTPS
  - ASA FirePOWER or dedicated standalone FirePOWER appliances behind the edge ASA to block and control traffic on all ports/protocols

- Remote work force, mobile users
  - Cloud Web Security (CWS) for consistent security off-premise

Mixing on-premise with cloud might be the most secure approach.
Handling the Mobile Users
Mobile Users Security Landscape

- **VPN Technology Choices**
  - L2L IPSec FlexVPN
    - Remote Offices IOS Routers
    - Home Office – CVO (Cisco Virtual Office)
  - **AnyConnect Remote Access VPN**
    - Laptops, PCs
    - Smartphones, Tablets, BYOD
    - Clientless SSL VPN
      - Browser-based Remote Access
      - Web Portal access from anywhere

- **VPN Traffic Backhaul Patterns**
  - Bandwidth Conservation vs Protection

- **Site-to-site (L2L)**
  - Centralized HQ Internet Breakout
  - Spoke Direct Internet Access (DIA)

- **Mobile User Remote Access (RA)**
  - Full Tunnel
    - Centralized NGFW and WSA
  - Split tunnel
    - Centralized NGFW
    - Cloud-based CWS
  - No tunnel
    - Cloud-based CWS

---

BRKSEC-2881 VPN Remote Access with IOS & Introduction to FlexVPN

BRKSEC-3033 Advanced AnyConnect Deployment and Troubleshooting with ASA

BRKSEC-3053 Advanced Practical PKI for Remote Access VPN
NGFW VPN Traffic Backhaul

- **ASA with FirePOWER Services** acting as a Remote-Access VPN Headend
- **Multiple layers** of traffic protection:
  - FW ACLs, NGFW, Web Security, NGIPS, AMP
  - No SSL inspection today
- **AnyConnect 4.0 VPN Client**
  - IPSec IKEv2 or SSL VPN (DTLS-based)
- **All traffic tunneled** to HQ, no split-tunnel
  - Can enhance integrity with Always-On
  - Start-Before-Login (SBL) if applicable
- **ISE** can serve as a **centralized Policy Engine**
  - Apply Authorization Policies (VLAN, ACL)
  - TrustSec SGT imposition for Remote Users
    - ASA 9.2 Software with ISE 1.2
  - Posture integration with ASA RADIUS CoA support
    - AnyConnect 4.0 Unified NAC (Posture) Agent
WSA VPN Traffic Backhaul

- **ASA with FirePOWER Services** acting as a Remote-Access VPN Headend
  - AVC Visibility, NGIPS and AMP services on-box
  - Protection beyond Web provided already by WSA

- **WSA enabling comprehensive Web Security**
  - All the Secure Web Proxy capabilities discussed
  - Transparent or explicit deployment modes
  - WCCPv2 done by ASA or L3 switch
  - HTTPS decryption available
  - Advanced Malware Protection (AMP) on-box

- Known as the **AnyConnect Secure Mobility Deployment Model** or **MUS (Mobile User Security)**
  - Provides true SSO for Remote Users
  - ASA passes the VPN user identity to WSA
  - WSA does not need to perform authentication again

CWS Cloud Web Security

- **ASA with FirePOWER Services** acting as a Remote-Access VPN Headend
  - AVC Visibility, NGIPS and AMP services on-box
  - Protection beyond Web provided already by CWS
  - Web Traffic to CWS is split-tunneled, bypassing VPN

- **CWS enabling centralized Web Security**
  - Cloud-managed Secure Web Proxy
  - Outbreak Intelligence and Signature-Based
  - AMP Cognitive Threat Analytics (CTA)
  - HTTPS decryption available
  - Geographical High Availability

- **AnyConnect Web Security** module provides CWS traffic redirection independently
  - Protection with VPN established or disconnected
  - Supported with Windows, MacOSX
  - AnyConnect Profile Editor

Cloud Web Security for Remote Users @Cisco

- **Users off the VPN network**
  - AnyConnect Web Security Module
  - Cloud Web Security (CWS)
  - Redirect to the nearest CWS tower

- **Solution Effectiveness**
  - 1% of all outbound web traffic blocked
  - Over 80,000 objects *per day*

- **Encountered Threats on a daily basis**
  - Trojans, Spyware
  - Recently registered and unknown domains

- **Visibility**
  - Retrospective AMP and CTA Reporting

---

BRKSEC-2909 In search of the Silver Bullet for protection against web-based malware using Cloud Web Security
The Encrypted Traffic Challenge
SSL and Content Filtering at Internet Edge

Problem Definition

- Primary goal of SSL was to achieve **Confidentiality at Internet Scale**
  - Initial implementations date back to the early 90's
  - Operates above TCP/IP but below application layer (session layer)
  - Establishes a secure channel to transmit other protocol data
    - HTTP over SSL = HTTPS
    - FTP over SSL = FTPS
  - SSL hides the web content we would like to filter
    - HTTP protocol messages completely encrypted
    - Content and payload hidden as well
  - SSL Encryption of web application traffic becoming the new normal
    - SSL around 25-30% of typical Enterprise web traffic and growing rapidly
    - Salesforce, Office 365, Facebook, Twitter, Gmail
  - Attackers increasingly using SSL encryption to bypass detection
    - Zeus encrypted file download and subsequent encrypted data exfiltration
No SSL Decryption and Content Filtering

What can we achieve **without decrypting** the traffic?

- **Server Name Indication:** Optional TLS extension that indicates the HOSTNAME of the server being requested.

- **Subject and Subject Alternate Names:** Fields in the Certificate that identify the server hostname (FQDNs).

- Cannot filter HTTP request and content, since it is encrypted.
SSL Decryption Options: FirePOWER Appliances

Standalone FirePOWER (7000, 8000) devices can now natively identify SSL and decrypt the traffic before applying NGFW, NGIPS and AMP capabilities.

- Multiple Deployment modes
  - Inbound passive (with known keys)
  - Inbound inline (with or without keys)
  - Outbound inline (without keys)

- SSL support for HTTPS & StartTLS based applications
  - SMTP, POP, FTP, IMAP, Telnet

- Centralized enforcement of SSL certificate policies
  - Blocking self-signed encrypted traffic, SSL version, specific Cipher Suites, unapproved mobile devices
Outbound Inline SSL and Content Filtering

Man in the Middle (MitM) Decryption with FirePOWER Standalone Appliance 5.4 Software
SSL Decryption Options: WSA

SSL Decryption with Web Security Appliance (WSA).

- Supported in Transparent and Explicit Modes
  - In transparent, no access to client headers
  - In Explicit, URL and Destination Port in headers
- Decryption Policies specify what traffic should be decrypted and further inspected:
  - Reputation Score (WBRS), URL Category
- Policy Actions
  - Pass Through, Monitor, Decrypt, Drop
- HTTPS Proxy Decryption Options
  - Decrypt for Authentication, Application Detection (AVC)
  - Decrypt for End User Notification (EUN) and Acknowledgment
- Invalid Certificate Handling (Drop, Decrypt, Monitor)
- Certificate Revocation with CRL and OCSP
- Decryption takes precedence over Access policy
SSL Decryption with CWS

HTTPS Inspection with Cloud Web Security

- Server Host name read with HTTPS Certificate Grabber with no decryption enabled
- Standard User Notification that traffic is decrypted
- CWS CA Certificate generation options:
  - SSL certificate in ScanCenter, Cisco will be the Certificate Authority (CA)
  - Enterprise CA, generate CSR in the ScanCenter Portal
- Differentiate traffic to decrypt
  - URL Categories, Web Applications (AVC)
  - Domains, Networks/IPs
- Application Decryption can be enabled separately for AVC
- Can allow user to continue if certificate error
  - Expired, Invalid, Revoked
Outbound CWS HTTPS Decryption Flow

CONNECT request (+ CWS headers)

200-OK in response to connect

ClientHello SSL handshake from browser

Cert trusted by browser; Downstream handshake

HTTP Request (encrypted)

Apply web filtering policy

Scan content for threats

Filtered HTTP Request (encrypted)

Company/User authentication

Is the HTTPS server answering?

Get SNI from handshake
Process SNI or Host/IP from CONNECT headers to determine if HTTPS inspection is required

Inspection required: Initiate new SSL handshake

Use SSL certificate to create new cert signed by us
SSL Decryption End-User Experience

- When choosing what to decrypt, think about:
  - Breaking trust
  - The user experience
- Decrypting only what is necessary
- Use your existing PKI infrastructure
- Push certificate out via GPO/Scripts
- Not every Application or Device has a modifiable trust store
Let’s Encrypt is just around the corner

Let’s Encrypt is a new Certificate Authority:

It’s **free, automated, and open**.

Arriving Summer 2015

https://letsencrypt.org/
Encrypted traffic inspection summary

Technology Choices Available

- Require integrated NGIPS/NGFW/AMP appliance
  - FirePOWER Physical Appliances (7000 and 8000 series) with 5.4 Software

- Only SSL Decryption needed, purpose-built device
  - Standalone SSL Decryption Appliance

- Focus on Secure Web Proxy on-box HTTPS Decryption
  - Web Security Appliance (WSA)

- Remote work force, mobile users, HTTPS Decryption in the Cloud
  - Cloud Web Security (CWS) for consistent security off-premise

- Understand impact of SSL Decryption in integrated use cases
  - Up to 90% performance hit with 50% decrypted traffic volume

BRKSEC-2525 Network Impacts of HTTPS Transport Encryption

It is your responsibility to determine privacy laws for decryption.
Don’t Be a Phish –
Employing Email Security
Internet Edge Email Security

The Fatal Assumptions:

1. Email is a **thing of the past**
   - Most of advanced threats start with email

2. I **understand my email flows**
   - Machines that can send and receive mail

3. I am a **good Internet citizen**
   - Utilizing DNS-based validation

4. I am **protected** from the SPAM
   - Combating threats, including blended attacks with multiple layers of defense

5. My **users have been trained** to identify malicious email
   - Technology is no substitute for **awareness**
Malicious actors steal valid email credentials from users with malicious spam messages
- Then send spam from compromised, yet *reputable*, accounts.

Spam is now more dangerous and **very hard to detect**
- **Highly-targeted**, low-volume spam messages enjoy high/no reputation
- Malicious spam is the first step (phishing email) in a **blended attack**

Spam volumes have increased **250%** from January through November 2014 (100 Billion / Month)
Anatomy of an APT Attack

1. **Infiltration and Backdoor establishment**
   - Attackers may use social engineering or exploit vulnerabilities to gain initial access to the network.

2. **Reconnaissance and Network Traversal**
   - Attackers gather information about the network and its resources.

3. **Exploitation and Privilege Elevation**
   - Attackers exploit vulnerabilities to gain higher privileges within the network.

4. **Staging and Persistence (Repeat 2,3,4)**
   - Attackers establish a foothold and maintain access to the network.

5. **Data Exfiltration**
   - Attackers steal sensitive data from the network.

Diagram:
- **Perimeter (Inbound)**
- **Perimeter (Outbound)**
- **C2 Server**
- **Admin Node**
- **Data Exfiltration**
Email Security Options: ESA

Email Security Appliance (ESA)
- Purpose-Built AsyncOS Physical/Virtual Appliance
- Speaks SMTP, ESMTP, SMTP over TLS
- High Availability with DNS, Clustering, Load-balancers
- Email domain reputation with senderbase.org (SBRS)
- Multiple Anti-Spam Engines (IPAS, Cloudmark, IMS)
- Web Reputation (WBRS), URL filtering for email content
- Virus Outbreak Filters (OF)
- Multiple Antivirus Engines on-box (Sophos, McAfee)
- Advanced Malware Protection (AMP)
- Advanced Domain Validation: SPF, DKIM, DMARC
- On-box RSA DLP Engine
- External RSA Enterprise Manager DLP integration
- CRES-based Email Encryption Service (PXE)
- On-box GUI or SMA centralized management
Email Security Workflow

On-premise ESA email flow:

1. Sender sends email to user@companyX.com
2. What is IP for CompanyX Mail Server (MX and A record DNS Lookup)
3. IP Address for CompanyX email is a.b.c.d (ESA)
4. Mail Server sends the email to ESA (SMTP)
5. After inspection, email is sent to company groupware Mail Server
6. Employee retrieves the cleaned email
ESA Direct Internet Dual Interface Attach:

- Easy to deploy
- The ESA is hardened out-of-the box
- No protection for the inside network or outside interfaces
- ESA production interfaces directly exposed
  - to the public Internet
  - to the Inside Networks
- ASA Firewall/NGIPS is not used to protect ESA
- Security nightmare. DO NOT DO scenario.
ESA Deployment: Protected Private Interface

ESA Direct Internet Protected Private Attach:

- Easy to deploy
- The ESA is hardened out-of-the box
- No protection for the outside interface
- ESA production interface directly exposed
  - to the public Internet
- ASA Firewall/NGIPS is not used to protect ESA public interface
- Minimally better, not recommended
- Security nightmare. DO NOT DO scenario.
ESA Deployment: Protected Public Interface

ESA Direct Private Protected Public Attach:
- Easy to deploy
- The ESA is hardened out-of-the box
- ESA production interface directly exposed
  - to the Inside Networks
- ASA Firewall/NGIPS used to protect ESA public interface
- Used in some deployments
- Even better than previous, still not recommended
- Not considered Highly Secure
ESA Deployment: Protected Single Interface

ESA Single Interface DMZ Attach:
- ASA Firewall/NGIPS used to protect ESA
- Simplifies firewall configuration for passing email related traffic
- No specific routes required on the ESA. Minimizes network troubleshooting
- Single interface represents a possible single point of failure or bottleneck
- Preferred and THE most common method of installation by customers
ESA Deployment: Protected Dual Interface

ESA Dual Interface DMZ Attach:
- ASA Firewall/NGIPS used to protect ESA inside and outside interfaces
- Simplifies firewall configuration for passing email related traffic
- Static routes required on the ESA
- Firewall represents a possible single point of failure or bottleneck
ESA Deployment: Cascaded Dual Interface

ESA Cascaded Dual DMZ Attach:

- Cascaded Firewall/NGIPS used to protect ESA inside and outside interfaces
- Simplifies firewall configuration for passing email related traffic
- Static routes required on the ESA
- Firewalls represent a possible single point of failure or bottleneck
- Larger deployments with dual-firewall strategy
ESA Deployment: Management Network

ESA **Separate Management** Network

- Meets the most stringent connectivity needs
- Requires a larger physical appliance with 3 interfaces or virtual appliance
- Applicable to all recommended ESA deployment models
- Use the route command via CLI to configure traffic flows for the extra interfaces
- **SMA Management Appliance** (physical/virtual) resides in the Management Network
Email Security **High Availability**:  
- Use larger Appliances with RAID and redundant PSUs  
- Configure NIC Teaming  
- Utilize ESA Clustering for config sharing  
- Configure multiple MX DNS Records  
- Employ Geographical ESA Redundancy  
- Deploy multiple ESA instances  
  ▪ ESAv and SMAv greatly helps  
  ▪ Mixing physical and virtual appliances  
- Utilize SMA(v) for centralized features

For even **larger scale**, use hardware or virtual loadbalancers with ESA(v) farm.
Achieving High Security with ESA

- Utilize Email **Reputation Filters** (SBRS) and Outbreak Filters (OF)
- Develop flexible **Content Filters** for powerful decision flows
- Use Multiple **Anti-Spam Engines** (IPAS, Cloudmark, IMS)
- Configure URL **Web Reputation** Filters to combat blended threats
  - For secure email message rewrite
  - For enforcing Web Acceptable Use Policies (AUP) to the email flows
- Apply **Rate Limiting** to identify compromised hosts
- Make use of **DLP Engine** for intellectual property, on or off-box options
- Be a **good Internet Citizen**, utilize SPF, DKIM and DMARC
- Enhance Enterprise integrity with **outbound email encryption** (PXE with CRES)
  - S/MIME is a new option
- Use multiple real-time **Malware Scanning** Engines (AV/AM)
  - Sophos and McAfee
- Employ **Advanced Malware Protection** (AMP)
  - File Reputation, Sandboxing and Retrospection
Cisco Registered Envelope Service (CRES)

1. Gateway encrypts message.
2. Recipient opens PXE message in web browser.
3. User authenticates & gets message key.
4. Decrypted message displayed.

Password

---

BRKSEC-3127 Advanced Dive Into Cisco’s E-mail Encryption Capabilities
Email Security Appliance AsyncOS 8.5
New Features and Enhancements

- **Advanced Malware Protection** (AMP) phase I
  - AMP sits between AV and Content Filters in the Mail Flow Pipeline

- **Web Reputation** and Web Category Integration

- Domain-based Message Authentication, Reporting & Conformance (DMARC) Support

- **Efficacy Enhancements** – Stochastic Sampling
  - False Positives Reduction

- Import-Export for Clusters

- **Bulk / Marketing Email** – a **High Volume Mail Management**
Email Security Appliance AsyncOS 9.0
New Features and Enhancements

• **Advanced Malware Protection (AMP) phase II**
  – Extended file type support:
    ▪ Windows PE executables
    ▪ Microsoft Office (new Open XML, old MSOLE2) and PDF
    ▪ Archive files: ZIP, TGZ, 7z, RAR, TAR and GZIP
  – Dynamic File Analysis Quarantine

  ▪ **RESTful API**
    – Stateless, HTTP/REST and JSON, HTTPS + Basic Auth
    – System Health and Report Data

  ▪ **S/MIME** Signing/Encryption (RFC 3369, 3370, 3850, and 3851)

  ▪ Flexible Policy Conditions: based on both sender and recipient

  ▪ Efficacy Enhancements – **Anti-Snowshoe campaign**

  ▪ Scale with **256 virtual gateways** for granularity and outbound mail campaigns
Email Security – is it still important? @Cisco

- 93% of all inbound mail dropped as SPAM by ESA reputation engine
- Additional blocks done inline with Cisco AMP (attachment scanning)
- All the major advanced attacks to hit Cisco have started via e-mail
- Everything is logged centrally for further incident investigation
### Emails delivered

<table>
<thead>
<tr>
<th></th>
<th>Emails / mo</th>
<th>Emails / day</th>
<th>Emails / employee / day</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted</td>
<td>124 M</td>
<td>5.6 M</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>Blocked</td>
<td>77 M</td>
<td>3.5 M</td>
<td>46</td>
<td>63%</td>
</tr>
<tr>
<td>Delivered</td>
<td>37 M</td>
<td>1.7 M</td>
<td>22</td>
<td>30%</td>
</tr>
<tr>
<td>Delivered, marked “Marketing”</td>
<td>9 M</td>
<td>0.4 M</td>
<td>5</td>
<td>7%</td>
</tr>
</tbody>
</table>

### ESA Blocked Emails

<table>
<thead>
<tr>
<th>ESA Blocked Emails</th>
<th>Emails* / mo</th>
<th>Emails / day</th>
<th>Emails / employee / day</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>By reputation</td>
<td>73 M</td>
<td>3.3 M</td>
<td>43</td>
<td>94%</td>
</tr>
<tr>
<td>By spam content</td>
<td>4.3 M</td>
<td>0.2 M</td>
<td>3</td>
<td>5%</td>
</tr>
<tr>
<td>By invalid receipts</td>
<td>0.4 M</td>
<td>0.02 M</td>
<td>0.25</td>
<td>1%</td>
</tr>
</tbody>
</table>

3.5M Emails blocked each day
„My opinion is that any company which does not know where their SMTP servers are, has to commit seppuku in front of the building starting from CIO. DNS administrators can prove their loyalty by cutting one finger from their right hand. ”

Member of Messaging Support Team
Very Large Global Corporation,
A Cisco E-mail Security Customer
Internet Edge Email Security – Summary
Picking The Right Technology

One technology deployed in different ways:

- Require on-premise highly scalable email security solution
  - **ESA physical or virtual appliances** deployed in DMZ, employing a rich set of security features for Inbound, Outbound and Encryption
  - Optional **SMA** for centralized management, reporting, tracking and quarantine

- Looking for cloud Email Security or Hybrid Approach
  - **Cloud Email Security (CES)** solution for cloud email adopters (Office365)
  - Hybrid deployment for best of both worlds, mixing on-premise ESA and CES

- Additionally, when outbound **Email Encryption** desired
  - Cisco Registered Envelope Service (CRES) or S/MIME

Surprisingly, **Email** is on the rise as one of leading **threat vectors** today.
Combating Advanced Malware with AMP
“You can’t defend. You can’t prevent. The only thing you can do is detect and respond.”

Bruce Schneier
Security Guru
Advanced Malware Protection

The Fatal Assumptions:

1. I can handle advanced malware threats with my current solution
   - Zero-day malware and APTs are on the rise

2. I understand malware propagation patterns
   - Utilizing FireSIGHT AMP Network Trajectory

3. I am applying a holistic approach
   - AMP Everywhere across my environment

4. I acknowledge that 100% detection does not exist
   - Applying AMP Retrospective Analysis

BRKSEC-2139 Advanced Malware Protection (AMP)
AMP Technology Brief in One Slide

- AMP Client queries TALOS Cloud for **file disposition**, sending the file fingerprint
  - Standard SHA256 hash, proprietary SPERO and ETHOS with more metadata

- TALOS Cloud immediately returns a **disposition verdict**
  - Good, Malicious or Unknown. Good can be forwarded, Malicious immediately blocked

- If disposition Unknown, the Cloud can perform dynamic analysis of the full file
  - Sandboxing produces a detailed **Dynamic Analysis Report** with File Threat Score (Reputation) 0-100

- Based on analysis results, we can start detection and mitigation across the whole environment
  - Block the malware on all AMP-capable devices (Hardware and Virtual FirePOWER appliances, ASA with FirePOWER Services, WSA, ESA, CWS, standalone AMP appliances, AMP Endpoints) preventing further malware spread
  - Perform **Retrospective** Analysis and visualize Network and Host **Trajectories** of the malicious file, enabling Malware Analysis, **Forensics** and Incident Response across the whole enterprise, **Internet Edge included**
AMP for Network Appliances

- **Network AMP** coherently available with:
  - FirePOWER NGFW/NGIPS Appliances (HW/SW)
  - ASA FirePOWER Services (5500-X, 5585-X)
  - Dedicated AMP Hardware Appliances

- FireSIGHT Management Center enables:
  - **AMP File Policy Actions**
    - Malware Cloud Lookup
    - Malware Blocking
    - File Detection and Blocking
    - SPERO analysis for MSEXE
    - File Storing on-box for further forensics
    - Send to Dynamic Analysis for Sandboxing
    - Choosing Direction of Transfer (Upload/Download)
    - Choosing Application Protocol
  - **AMP Network File Trajectory** Visualization
  - **AMP Custom Detections** and Clean Lists
AMP for Web Security Appliance

- **AMP for WSA** phase I and II today:
  - Secure Web Proxy Use Case
  - Enhancing Security **beyond traditional AM/AV**
  - Sits in WSA processing pipeline after AM/AV
  - **Managed by the WSA GUI**, not FireSIGHT

- WSA with AMP enables:
  - File Reputation, Sandboxing, Retrospection
  - SHA256 and SPERO (WinPE) fingerprints
  - Detailed **Web Tracking** and Cloud Reports
  - AMP-specific **logs** in accesslogs, amp_log
AMP for Email Security Appliance

- **AMP for ESA** phase I and II (9.0):
  - Secure Email Gateway Use Case
  - Enhancing Security **beyond traditional AM/AV**
  - AMP sits **between AV and Content Filters**
  - Managed by the ESA GUI, not FireSIGHT

- **ESA with AMP enables**:
  - File Reputation, Sandboxing, Retrospection
  - SHA256 and SPERO (WinPE) fingerprints
  - Native Dynamic **File Analysis Quarantine**
    - No Content Filters and Policy Quarantine needed
  - Detailed **Email Tracking** and Cloud Reports
  - AMP-specific **logs** in mail_logs, amp_log
Support for **AMP Private Cloud** Virtual Appliance
- AMP Private Cloud Virtual Appliance instance in the Internal Network
- Can be used for file disposition lookup and AMP for Endpoints Event Feeds

**Extended IoC** Support from AMP for Endpoints
- As new IoCs are made, FireSIGHT consume them
- They will appear in host profiles, IoC correlation
- IoC Examples
  - Multiple infected files detected by AMP for Endpoints
  - Microsoft calculator compromise detected by AMP for Endpoints
  - Multiple infected files detected by AMP for Endpoints

**Unicode** Filename Support
- Non-western character display in file names
Advanced Malware Protection – Summary
AMP Everywhere – an End-to-End Approach to Visibility

- **Network AMP** capabilities embedded in:
  - Standalone FirePOWER Appliances
  - ASA FirePOWER Services
  - Standalone Dedicated AMP appliances
  - Web Security Appliance (WSA)
  - Email Security Appliance (ESA)
  - Cloud Web Security (CWS)

- **Endpoint AMP** for:
  - Windows, MAC OS X
  - Android Mobile Devices

- **AMP Threat Grid** Platform for Unified Malware Analysis and Intelligence
  - On-Premise Appliances
  - Cloud-Based Portal
Leveraging the Context-Awareness
Active Authentication with WSA

Basic Authentication approach:
- User will be prompted for credentials
- WSA consults AD server using LDAP
- Slightly different with explicit and transparent
- Works with HTTPS
- Avoid, **nobody likes** to type in passwords

Active Authentication Workflow with WSA:
1. Unauthenticated user browses through WSA
2. WSA redirects user via HTTP Redirect to WSA IP
3. Browser connects direct to WSA
4. WSA sends HTTP Auth Request (401|407)
5. User authenticates
6. WSA sends HTTP Redirect to original URL (307)
7. Authenticated user browses through WSA
Passive Identity with CDA | SFUA

There are two standalone AD Connectors:

- **CDA** (Context-Directory Agent) for WSA, CX, ASA
  - Hardened Linux VM delivered as .iso file
  - WSA and legacy ASA-CX use CDA for TUI with AD
  - ASA uses CDA for user-based ACLs with IDFW

- **SFUA** (Sourcefire User Agent) for FirePOWER
  - Windows binary, Server and Workstation install
  - FirePOWER uses SFUA for TUI with AD

Passive Identity Workflow with NGFW:
1. AD User Logon Event
2. User Logon Event in Security Log (WMI)
3. Logged-in Domain User to IP Mapping (RADIUS)
4. Domain User and Group information (LDAP)
5. Traffic filtered by NGFW Access Policies
Native ISE and CDA integration
- CDA becomes broker for **AD and non-AD Users**
- ISE Configured to forward Syslog to CDA
  - AAA Audit, Passed Authentications and RADIUS Accounting Logs
- CDA Configured with ISE as a Syslog Server

Passive Identity Workflow with ISE and CDA:
1. User Authenticates against ISE with AD
   - 802.1X Wired or Wireless User
2. ISE sends Syslog with User-IP mapping to CDA
3. WSA consumes User-IP mapping from CDA
4. User Requests Webpage
   - WSA Transparent User Identification (TUI)
   - Web request proxied and enforced based on the WSA User-based Policy

CDA Installation and Configuration: [https://www.youtube.com/watch?v=rp_CpeILpNU](https://www.youtube.com/watch?v=rp_CpeILpNU)
Passive Identity with ISE and pxGrid

Major step in Context-Aware Security

ISE is the broker and ultimate source of truth
- pxGrid framework available already in ISE 1.3
- Ecosystem partners for context sharing (SIEM)
- ISE shares context using pxGrid with consumer devices
- Consumer devices get user-IP identity mappings and more

Work in progress
- WSA in preview, FirePOWER on roadmap

Passive Identity Flow with ISE and pxGrid:
1. User authenticates against ISE (802.1X)
   • Can be a Wired, Wireless or RA VPN user
2. Consumer device gets the user binding
3. Consumer device enforces access policy
   • Content filtering is based on the user identity

pxGrid API @Cisco Developer Community Portal (DevNet): https://developer.cisco.com/site/pxgrid/
# User Identity for Attribution @Cisco

<table>
<thead>
<tr>
<th>Source</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>IP assignments to machine, MAC address</td>
</tr>
<tr>
<td>VPN Headend</td>
<td>IP assignments to <strong>user</strong>, WAN address</td>
</tr>
<tr>
<td>NAT Gateway</td>
<td>IP assignment translation to RFC 1918, NAT Stitching</td>
</tr>
<tr>
<td>ISE</td>
<td>IP assignment to <strong>user</strong>, MAC address</td>
</tr>
</tbody>
</table>

[Diagram showing various components and connections, including DHCP, ISE, NAT, and VPN.]
There are many ways to identify the user:

- WSA Active Authentication (Basic)
- WSA SSO with NTLMSSP and Kerberos
- Transparent (Passive) User Identity (TUI)
  - WSA, ASA Passive Identity with CDA and AD (WMI), CDA and ISE (syslog)
  - FirePOWER Passive Identity with SFUA and AD
  - FireSIGHT Passive User Discovery with unencrypted protocols
    - AIM, IMAP, LDAP, Oracle, POP3 and SIP
- CWS has a broad set of Identity Mechanisms on its own
- ISE 1.3 with pxGrid is the strategic direction

**User Identity** is the key to **Attribution**, fundamental in Cyber Security.
Network Forensics for Apocalypse Prevention
Network Forensics with NetFlow

The Fatal Assumptions:

1. I am able to **understand my Traffic Flows**
   - Network Flow collection including Internet Edge
   - Unsampled NetFlow from my Infrastructure

2. I can indicate **unusual things** with NBAD
   - Context-Based Network-Based Anomaly Detection
   - Attackers, Victims, Behavior

3. I am catching the **Insider Threats**
   - Accidental, Intentional and the poor Victims

4. I am handling the **Indicators of Compromise**
   - With Cyber Threat Defense Solution (CTD)
   - Integrating with ISE for Attribution

**BRKSEC-2136** Preventing Armageddon: Finding the threat before its too late
Understanding Internet Edge Traffic Patterns
Making use of the Internet Edge Traffic Patterns

- Source and Destination Address (IPv4/IPv6)
- Source and Destination Port
  - Protocol, Application
  - DSCP
  - Ingress Interface
  - BGP Next-Hop Field
  - MPLS label Info
  - Multicast Info
  - L2 information (802.1q tag, CoS field, etc)
NetFlow Technology Brief

- Standards-based Flow Technology, with a long history (90’s, IOS 11.x)
  - NFv5, NFv9, IPFIX, NSEL, FNF (Flexible NetFlow)
  - Both Data Format and Protocol to transport the Flow Information from Exporter to Collector
  - Exported Creates Cache Entry based on Key Fields, exports expired/terminated flows to Collector
  - Configuration Defined by Flow Record, Exporter, Flow Monitor and Device Interface
  - Efficient, Low Overhead, Binary Format, many (20-50) flow records per packet

- Supported by the majority of the network Infrastructure, but mileage may greatly vary
  - IOS/-XE/-XR Routers, Catalyst and Nexus Switches
  - ASA provides NSEL (NetFlow Security Event Logging) support – state-based with NAT stitching

- If cannot export natively – generate with SPAN-attached appliance
  - Cisco NetFlow Generation Appliance (NGA)
  - Lancope FlowSensor Appliance (FS)

- For Network Forensics and Behavioral Anomaly Detection, unsampled (1:1) NetFlow
  - Sampled NetFlow still useful for traffic accounting, billing, understanding protocol mix, network planning

- NetFlow instrumentation is the foundation for Traceback and Attribution
- New security use for a very well-known technology

Network-Based Anomaly Detection (NBAD)

- **Host Group Targeted Reporting** unveils Network and Application traffic patterns

- **Concern Index** tracks hosts appearing to compromise the network integrity
  - New York, Desktops 10.50.100.83 190,075,544 1,901% High Concern Index, High File Sharing Index, High Total Traffic Ping, Rejects, TCP_Scan

- **File Sharing Index** indicates a peer-to-peer host activity
  - Atlanta, Trusted Wireless 10.10.200.59 180,385 361% High Concern Index, High File Sharing Index, High Total Traffic Ping, Ping_Scan, Port_Scan, TCP_Scan, TCP_Stealth

- **Target Index** visualizes hosts appearing to be victims of suspicious behaviour
  - Domain Controllers, Atlanta, DNS Servers, NTP Servers 10.10.30.15 118,019,003 11,802% Excess_Clients, Rejects
Catching the Insider Threats with CTD

**Unauthorized Access** violation attempted, denied by the Firewall

- **Internal Reconnaissance** Concern Index Event, scanning on tcp/445
  - Apr 17, 2013 12:39:57 AM (22 hours 7 minutes 4s ago)
  - Apr 17, 2013 10:40:06 PM (6 minutes 55s ago)
  - Atlanta, Engineer
  - 10.202.0.24
  - Addr_Scan/tcp-445(11380)

**Data Exfiltration** – identify suspicious transfers through Internet Edge over a long time

- **Data Hoarding** – transferring an large amount of data through the network
  - **Suspect** Data Hoarding – host **downloading** inbound from many hosts
  - **Target** Data Hoarding – host **uploading** unusual amount outbound to multiple hosts

- Target Data Hoarding: Yes
- None

- Tolerance: Never trigger alarm when less than: **500M** downloaded payload bytes in 24 hours
- Always trigger alarm when greater than: **1T** downloaded payload bytes in 24 hours

None
Handling the Indicators of Compromise (IoCs)

- Identify Suspected **Malware Infected Hosts** in the Client Host Groups

| 10.50.100.83 | POS Terminals | 199.188.204.182 | United States | 38s | FTP | 2.2k |

- Visualize the Malware Infection Spread with **Worm Tracker**
  - Primary and Secondary Infections
  - Subnets being scanned

- Apply Context-Aware Telemetry from **ISE** to understand the affected Users

| Jun 10, 2013 11:27:37 PM (8 days 20 hours 26 minutes ago) | Current | bmcmaison | 00:0f:1b:80:0f:27 (Iomega Corporation) | Windows7-Workstation | LC | Unknown Exporter (10.10.1.1) | GigabitEthermet5/37 |

- Investigate all the **Hosts Touched** by the originally Infected Host

Cyber Threat Defense with NetFlow @Cisco

- Flow collectors deployed globally
- **15 Billion flows daily** at Cisco
- Lancope Stealthwatch
- Ad-hoc searching
- Network forensics
- Analysis and Alarming
  - Suspected Data Loss
  - File Sharing
  - Large Number of Flows
  - C2 Discovery
1. **Detect host** communicating with external Command-and-Control

2. Investigate **other internal hosts** communicating with the same C2

3. Uncover **other malicious external entities** from the compromised hosts
“The user's going to pick dancing pigs over security every time.”

Bruce Schneier
Security Guru
Incident Response Tools – Detection and Mitigation
Egress Detection Topology Example @Cisco

- Extensible and modular topology focused on the **Internet Edge egress** traffic
- Compromised hosts will try to establish **call-home** connections
- Security **data logging** is the key
- Fundamental Incident Response Tool
Massively Scalable Log Architecture:
- Global Search
- Regional Storage
- Redundant Forwarding
- Splunk, Kibana, Apache

Multiple Data Sources:
- Intrusion Detection Systems (IDS/IPS)
- NetFlow Network Devices
- Web Proxy logs (WSA)
- Email gateway logs (ESA)
- DNS and other logs
Cisco WSA and Splunk @Cisco
Data scale **per day** of operations:
- 22TB of network traffic inspected
- 1TB of data (average) logged and indexed
- 8 Billion web objects proxied
- 2.5 Billion DNS requests logged
Passive DNS @Cisco

- DNS is a **critical** Internet Service
- CSIRT logs **2.5 Billion DNS queries/day**
- DNS queries and answers helps to:
  - understand what the users machines want to know
  - discover attacks
- DNS Data Logged **unveils trasures:**
  - New domains (less than a week old)
  - Fast Flux domains (multiple IPs, short TTL)
  - Esoteric domains (uniqueness, random generation)
  - DDNS domains
  - Lookup Failures
  - Spikes in DNS traffic
  - C2 Servers hardcoded in malware
- **Correlate** with NetFlow, Packet Capture and Application Logs

\[\text{Src/Dst} \quad \text{qname/nbname} \quad \text{qtype/nbtype} \quad \text{NetBIOS suffix}\]
Understanding DNS Response Policy Zones (RPZ)

- Works with **BIND DNS services**
- Near real-time **blocking and monitoring**.
- Can be **scripted** to automatically block domains from a list or feed.
- Log data is extremely valuable
- Currently have the following implemented:
  - **NXDOMAIN** – Returns non-existent domain. Block, but don’t send user to sinkhole. E.g. Dynamic DNS providers.
  - **NODATA** – Returns Nothing
  - **LOCAL DATA** – Returns a “walled garden” IP. Sinkhole
    - Captures common protocols – HTTP, SMTP, IMAP, POP
    - As useful as web proxy logs (captures referrer, full URL, UA, etc)
    - Can be built to capture entire payload
  - **NO-OP** – Whitelist. Allows subdomain exception to blocked domain *example.com is firewalled

<table>
<thead>
<tr>
<th>POLICY</th>
<th>SYNTAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXDOMAIN</td>
<td>badsite.com.rpz.mycompany.com CNAME .</td>
</tr>
<tr>
<td>NODATA</td>
<td><a href="http://www.badsite.com.rpz.mycompany.com">www.badsite.com.rpz.mycompany.com</a> CNAME <em>.</em></td>
</tr>
<tr>
<td>Local Data</td>
<td>badsite.com A 192.168.7.77</td>
</tr>
<tr>
<td>NO-OP</td>
<td>good.example.com CNAME good.example.com</td>
</tr>
</tbody>
</table>


Mitigation with DNS RPZ @Cisco

malicious-domain.com
Is BAD!

External DNS RPZ

someotherwebsite.com
LOCAL RPZ

Corporate DNS Server

DNS Query
malicious-domain.com

DNS Query
someotherwebsite.com

DNS Response
from DNS RPZ

Client

Upstream DNS Server

example.com is 93.184.216.119

Where is example.com?

Policy Quarantine with ISE EPS Services
Dramatically reducing time to contain incidents

- Utilizing the EPS (Endpoint Protection Services), known as ANC – Adaptive Network Control
- One of the most unknown and underused ISE capabilities
- ISE servers can globally keep Host MAC address in a restricted zone
- Infected Hosts can still have access to remediation tools, while not affecting other systems
- Quarantine / Unquarantine can be manual or automated (API-driven)
Utilizing Open Source Security Projects
Snort 2.9.7 and Snort 3.0 Alpha available

- https://snort.org/

- The most widely deployed Open Source IPS system in the world
Snort Architecture

- **Packet Decoder**
  - Packets are read using the *Data AcQuisition library* (DAQ) (e.g. `afpacket`)
  - Decodes datalink protocols
  - Decodes network protocols
  - Decodes transport protocols

- **Preprocessors**
  - Examine packets
  - Modify packets
  - Normalize traffic

- **Detection Engine**
  - Uses Snort rules to create signatures for threats
  - Wide range of detection capabilities
  - Modular detection elements
An open source application-focused detection language that enables users to create, share and implement custom application detections (AVC)

– Preprocessor for Snort, available in 2.9.7
– Identifies application and generates appid attributes that can be used in Snort rules
– Currently 3800+ application and protocol definitions available
– Lua to create own application detectors http://www.lua.org
  ▪ Lua is a powerful, fast, lightweight, embeddable scripting language.
  ▪ Simple, and small – under Linux, interpreter is 182K, libraries 244K
– Leverages Snort HTTP preprocessor for header extraction
– Generates application statistics in Uniform2 format
  ▪ Statistics file can be read (u2openappid | u2spewfoo)
  ▪ Statistics can be forwarded to Syslog server (u2streamer)
  ▪ Reports and application names in logs
– Application blocking
– To be incorporated into FirePOWER technology
Building an Open Source NGFW with OpenAppID

Because, Why not?

Next-Generation Firewall (NGFW) defined as FW + AVC + IPS

http://blog.snort.org/2014/03/openappid-install-video.html

https://www.youtube.com/watch?v=xXAYEimXp8A
ClamAV
http://www.clamav.net/

- Open source (GPL) **Antivirus Engine** for detecting trojans, viruses and malware
  - The standard for **Mail Gateway**, Sendmail integration
    - Supports Web Scanning and Endpoint Security
  - **High Performance** multi-threaded scanner daemon
  - Command line utilities for on demand file scanning
  - Automatic signature **updates**
  - Multiple file formats, file and **archive** unpacking
    - Zip, RAR, Dmg, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS and others
  - Built-in support for ELF **executables** and Portable Executable files
    - UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack and obfuscated with SUE, Y0da Cryptor
  - Built-in support for popular **document formats**
    - MS Office and MacOffice files, HTML, Flash, RTF and PDF
  - Multiple **signature languages**
OpenIoC

- Open Framework developed by Mandiant
- Extensible XML Schema, more than 500 attributes
  - [http://openioc.org/terms/Current.iocterms](http://openioc.org/terms/Current.iocterms)
- IoC Definition is a **logical sentence** using attributes:
  (registry key AND file name) OR (log event)
- Incident Response Teams can create their **own detections**

(File MD5 is A35930B93D3057493EF3567395BC3C0F) ||
(Network DNS contains mybaddomain.net) ||
(((File Name is asdf.exe) && ((File Size is 35343) || (File Compile Time is 2008-09-29T00:24:05Z))) ||
  ((Service Name is svc24) && (Service DLL contains svc24_log.dll))

- Test IoCs for Stuxnet, Zeus, Duqu detection
- Community knowledge sharing
  - [https://www.iocbucket.com/](https://www.iocbucket.com/) and others
- Used in Endpoint AMP Cloud Console Today
  - More to come in the future

OpenSOC Project
„Analyzing 1.2Mpps in Real-Time”

- Big Data security analytics framework for a **massive scale DC**
- Consume, monitor **network** traffic and **machine exhaust** data
- Dedicated to **extensible and scalable** advanced **security analytics** tool
- Apache {Flume, Kafka, Storm, Hive, Hbase}, Elastic Search, Kibana, Hadoop
  - Extensible spouts and parsers for attaching OpenSOC to monitor **any telemetry source**
  - Extensible **enrichment** framework for any telemetry stream
  - **Anomaly detection** and real-time rules-based alerts for any telemetry stream
  - **Hadoop-backed storage** for telemetry stream with a customizable retention time
  - Automated real-time **indexing** for telemetry streams backed by Elastic Search
  - **Telemetry correlation** and SQL query capability for Hadoop data backed by Hive
  - ODBC/JDBC compatibility and integration with **existing analytics tools**

[http://www.slideshare.net/JamesSirota/cisco-opensoc](http://www.slideshare.net/JamesSirota/cisco-opensoc)
[https://www.youtube.com/watch?v=UKqjd4tg8o](https://www.youtube.com/watch?v=UKqjd4tg8o)
Summary
What We Have Discussed Today

Infrastructure and Protocols

Network Firewall

Next-Generation Firewall (NGFW)

Next-Generation IPS (NGIPS)

Web Security

Content Filtering

Mobile Users Remote Access

SSL Decryption and Inspection

Email Security

Advanced Malware Protection (AMP)

Identity Attribution

Network Forensics

Incident Response

Open Source Custom Tools

SUCCESS
Embracing the Holistic Threat Continuum

BEFORE
- Control
- Enforce
- Harden

DURING
- Detect
- Block
- Defend

AFTER
- Scope
- Contain
- Remediate

Infrastructure and Protocols
- Network Firewall
- Next-Generation Firewall (NGFW)
- Next-Generation IPS (NGIPS)

Web Security
- Content Filtering
- Email Security

Advanced Malware Protection (AMP)
- Network Forensics

Mobile Users
- Remote Access VPN

SSL Decryption and Inspection

Open Source
Custom Tools

Context-Awareness

Attribution
...BUT...
“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

Bruce Schneier
Security Guru