Network Segmentation – Pro’s and Con’s

Ken Kaminski (kkaminsk@cisco.com)
Cisco Systems
Technical Solutions Architect – Enterprise East
CISSP, GCIA, GPEN, GAWN, GCFA, GMOB
June 2016
Drivers for Network Segmentation
Segmentation Framework
Identity and Trust
Policy Enforcement
Trustsec Software Defined Microsegmentation
Visibility
Future of Network Segmentation
Nomenclature: The definition of segmentation

segmentation
/ˌsɛɡmɛnˈteɪʃən/

1. The act or an instance of dividing into segments
2. 1650s, "a cutting in small pieces;"

http://dictionary.reference.com/browse/segmentation
Drivers for Network Segmentation
Factors governing segmentation

Line of business – BU segmentation

Payment Card Industry

Hospital Network

As networks evolve, granular segmentation is desired

Bring-Your-Own-Device

Mergers and Acquisitions

Multi-Tenancy
And yet this feels like only the beginning…

THE INTERNET OF THINGS AT WORK

As wearables and other connected devices increasingly make their way into the workplace, IT professionals still see more risk than benefit. Yet with sound preparation, education and governance, enterprises can be well-positioned to embrace the benefits of the Internet of Things (IoT).

INCREASED SECURITY THREATS — 49%

BIG CHALLENGES

DATA PRIVACY — 25%

IDENTITY AND ACCESS MANAGEMENT — 8%

COMPLIANCE REQUIREMENTS — 6%

OWNERSHIP OF TECH AND/OR DATA OUTSIDE OF IT — 6%

43% SAY ORGANIZATION ALREADY HAS OR EXPECTS TO CREATE PLANS FOR INTERNET OF THINGS WITHIN NEXT 12 MONTHS

60% BELIEVE “BRING YOUR OWN WEARABLE” AND “BRING YOUR OWN DEVICE” ARE EQUALLY RISKY
Preventing the spread and extent of compromise by limiting workstation-to-workstation communication is a critical component of a defense-in-depth strategy.
Targeted Attacks and Lateral Movement (Before Segmentation)

Research targets
1. C2 Server
2. Spear Phishing (you@example.com)

Victim clicks link unwittingly
Bot installed, back door established and receives commands from C2 server

Scan LAN for vulnerable hosts to exploit & find privileged users

Privileged account found

Lateral Movement (Scanning, Pivoting, Privilege Escalation, Brute Force, etc.)

System compromised and data breached.

Data exfiltrated

enterprise network
Lateral Movement

How Attackers Find Valuable Information

Overview of attacks

Among the many missing details of this breach, the attackers’ original point of entry into Target’s internal network is the most notable. Likewise, details about the attackers’ tactics, techniques, and procedures (TTPs) as they gained initial access and moved laterally through the network remain largely unknown. A

Home Depot said that the stolen vendor credentials did not give the hackers direct access to point-of-sale systems. More likely, the hackers were able to gain legitimate access to the Home Depot network through the vendor account and then pivot laterally until landing on the PoS system.

http://www.sec.gov/Archives/edgar/data/1598110/000119312515081968/d868623df1a.htm
Motivated Threat Actors Behind Breaches:

Regular Identity Theft Ave. Payout
$2,000

Medical Identity Theft Ave. Payout
$20,000

Social Security Ave. $1~

Credit Card Data $0.25-$60

Bank Account Info $1000+ depending on account type and balance

Full Identity Profile $500~

Medical Record $50+

Health Insurance Credential $20+

Source: EMC
“Good network and role segmentation will do wonders for containing an incident.”


“Segregate networks, limit allowed protocols usage and limit users’ excessive privileges.”

SANS CIS Critical Security Controls - # 1 Inventory of Authorized and Unauthorized Devices
PCI 3.0 11.3.4: Requires annual penetration tests to verify segmentation is operational and effective.
Segmentation Framework
Segmentation Framework and Security Zone Definition

- What parameters define a security zone?
  - Identity / Trust
  - Isolation
  - Policy Enforcement
  - Visibility
  - Availability / Dependencies

- Security Zone = \{Identity, Isolation, Policy Enforcement, Visibility, Availability\} tuple

- Broadly applicable model: HSA / DMZ design, SCADA separation, PCI bubbles, etc…
Effective segmentation comes from enabling foundational capabilities first: defining a Framework, and then enabling Identity and Visibility. Actual “segmentation” follows in the form of Isolation and Policy Enforcement.

Basically, you can’t manage what you can’t measure.

Note: Availability is not explicitly included but the assumption is that it addressed at every layer.
Segmentation: Controlling the threats

Micro Segmentation:
• Define segmentation policy within zones
• Ex: user to user policy

Segmentation:
• Define business critical/relevant zones
Security Determinants and Technology Examples

### Identity / Trust
- 802.1x and related
- VPN Authentication
- Secure Group Tags
- LISP
- IP Address
- MAC Address
- VM Identity, Endpoint Groups

### Policy Enforcement
- ACL’s (VLAN ACL / Router ACL / Port ACL)
- Firewall technologies (stateful ACLs and more)
- Application Layer Inspection: AppFW, WAF, etc.
- Intrusion Prevention Systems
- SGACL’s
- Network Functional Virtualization
- Automation

### Isolation
- Physical topology
- VLANs, WLANs & PVLANs
- VRFs, EVN, (MPLS)
- VDC’s, VPC’s, OTV
- [m]GRE / IPSec / DMVPN / GETVPN
- VXLAN (STT, NVGRE, NSH, etc.)
- Service Chaining

### Visibility
- NetFlow
- NG Intrusion Prevention Systems
- Breach Detection Systems
- ACL / FW / Proxy Logging
- Endhost Agent Logging
- Threat Intelligence
- Controller, Fabric, and Virtual Switch Statistics

### Availability [Dependencies]
Identity and Trust
Identity/Trust

- Multifactor Authentication
- 802.1x and related
- VPN Authentication
- Secure Group Tags (TrustSec)
- LISP
- IP Address
- MAC Address
Identity Engine Policy Server is a Standards-Based AAA Server
Access Control System Must Support All Connection Methods

Supports network vendor solutions via standard RADIUS, 802.1X, EAP, and VPN Protocols
Authentication and Authorization
What’s the Difference?

Who/what the endpoint is.

What the endpoint has access to.

802.1X / MAB / WebAuth

RADIUS

RADIUS

RADIUS

Authenticatio

Authorization
What is Profiling?

**Collection**
- NMAP
- DNS
- NetFlow
- HTTP UA
- SNMP
- CDP/LLDP
- Radius
- AD/Ext DB
- DHCP

- Process of collecting data to be used for identifying devices
- Uses Probes for collecting device attributes

**Classification**

Classifies based on Device fingerprint
Authorization Rules

- 802.1X / MAB / WebAuth

Return standard IETF RADIUS / 3rd-Party Vendor Specific Attributes (VSAs):
- ACLs (Filter-ID)
- VLANs (Tunnel-Private-Group-ID)
- Session-Timeout
- IP (Framed-IP-Address)
- Vendor-Specific including Cisco, Aruba, Juniper, etc.

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions (identity groups and other conditions)</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Profiled Cisco IP Phones</td>
<td>if Cisco-IP-Phone</td>
<td>then Cisco_IP_Phones</td>
</tr>
</tbody>
</table>


Policy Enforcement and Isolation
Traditional Segmentation

- Fundamentally VLAN based
- Every segment is a separate VLAN / Subnet / VRF
- Segment to segment communication governed by IP routes and IP based policies
- Classify assets in to VLAN, transport context in L2 (VLAN tag) / L3 (IP address / VRF), Enforce based on IP-ACLs
Authorization and Enforcement

**VLANS**
- Does not require switch port ACL management
- Preferred choice for path isolation
- Requires VLAN proliferation and IP refresh

**dACL or Named ACL**
- Less disruptive to endpoint (no IP address change required)
- Improved user experience
- Increased ACL management
Dynamic VLAN Assignment Issues

- Not recommend using different VLANs between pre-authentication and post-authentication because many endpoints (e.g. Mobile devices and OS X) do not have a good way to automatically refresh IP addresses upon VLAN changes. The problem with Mobile Devices is they do not support an IP refresh applet. It is still possible to assign these endpoints to a different VLAN that use the same subnet, but will have different policies based on upstream config on that VLAN. IP change should be steered away from whenever possible.

- Can return VLAN authorization, but the network device is not able to force IP refresh. Some workarounds include setting very short DHCP lease timers in the initial VLAN when user is in redirect state. If so, consider removing DHCP Profiling and ip helper on this subnet to avoid excessive DHCP updates to the device profiler, especially when final IP not yet applied.

- A problem with non-802.1x devices not capable of running a supplicant when using MAB. Device enters 1st vlan and then is profiled and moved to a second vlan. This only happens the first time the device connects – solution is pull the cable and reconnect after a few seconds.
Traditional Policy and Segmentation

Design needs to be replicated for floors, buildings, offices, and other facilities. Cost could be extremely high.
Traditional ACLs are High Overhead

- Adding destination Object
- Adding source Object

ACL for 3 source objects & 3 destination objects

Permit NY to SRV1 for HTTPS
Deny NY to SAP2 for SQL
Deny NY to SCM2 for SSH
Permit SF to SRV1 for HTTPS
Deny SF to SAP1 for SQL
Deny SF to SCM2 for SSH
Permit LA to SRV1 for HTTPS
Deny LA to SAP1 for SQL
Deny LA to SAP for SSH
Permit SJC to SRV1 for HTTPS
Deny SJC to SAP1 for SQL
Deny SJC to SCM2 for SSH
Permit NY to VDI for RDP
Deny SF to VDI for RDP
Deny LA to VDI for RDP
Deny SJC to VDI for RDP

Complex Task and High OPEX increases with number of source and destinations
Next Generation Firewalls (NGFW)

- Added Application Awareness, IPS, and User Identity (Identity Firewalling – AD/LDAP)
- **Caution** on Vendor Claims for Application identity – efficacy rates vary
- Encrypted traffic is ever increasing – decryption has severe performance implications
Stateful Firewalls in the Campus

Functional, but **OPEX Increases** as User/Device Groups Increase + **Performance Issues** on Firewall (1 to 10 to 40GB links)
Device Partitioning
Layer 2 vs. Layer 3 Virtualization

VLAN—Virtual LAN
- Virtualize at Layer 2 forwarding
- Associates to one or more L2 interfaces on switch
- Has its own MAC forwarding table and spanning-tree instance per VLAN
- Interconnect options?
  VLANs are extended via a physical cable or virtual 802.1q trunk

VRF—Virtual Routing and Forwarding
- Virtualize at Layer 3 forwarding
- Associates to one or more Layer 3 interfaces on router/switch
- Each VRF has its own Forwarding table
  Routing process (RIP, EIGRP, OSPF, BGP)
  Interfaces
Enterprise Network Virtualization
Key Building Blocks

Device Partitioning

“Virtualizing” the Routing and Forwarding of the Device

Virtualized Interconnect

Extending and Maintaining the “Virtualized” Devices/Pools over Any Media
- Defined router supports **routing (RIB)**, **forwarding (FIB)**, and **interface per VRF**
- Leverages “Virtual” **encapsulation** for separation:
  - Ethernet/802.1Q, GRE, Frame Relay
  - 802.1q different vlan per hop: VRF-Lite vs one vlan through infrastructure: EVN
- The **routing protocol** is also “VRF aware”
- Layer 3 VRF interfaces cannot belong to more than a single VRF
Path Isolation

Data path virtualization

• Hop-by-Hop - VRF-Lite End-to-End
• Multi-Hop - VRF-Lite GRE
• MPLS-VPN
• MPLS VPN over IP
• MPLS VPN over DMVPN
• MPLS VPN o GRE/mGRE
# Network Virtualization Technique Comparison Chart

<table>
<thead>
<tr>
<th></th>
<th>Multi-VRF (Hop-by-Hop VN)</th>
<th>EVN (Hop-by-Hop VN)</th>
<th>MPLS (Edge-to-Edge VN)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Design</strong></td>
<td>Small to mid-size networks based on VN scalability requirements</td>
<td></td>
<td>Large size</td>
</tr>
<tr>
<td><strong>VN Scale Limit</strong></td>
<td>8¹</td>
<td>32</td>
<td>4000</td>
</tr>
<tr>
<td><strong>Technology Integration</strong></td>
<td>Non-disruptive—No design and infrastructure change required.</td>
<td>Disruptive—No design change but requires EVN-capable hardware and software.</td>
<td>Disruptive—Requires MPLS-capable core and edge systems.</td>
</tr>
<tr>
<td><strong>Global Infrastructure</strong></td>
<td>IP-based</td>
<td></td>
<td>IP/MPLS-based</td>
</tr>
<tr>
<td><strong>Operational Complexity</strong></td>
<td>Simple. Complex as network expands.</td>
<td>Simple</td>
<td>Complex, Minimized with simplified network design.</td>
</tr>
<tr>
<td><strong>VN Manageability</strong></td>
<td>Disruptive—Requires hop-by-hop VN provisioning. However EVN simplifies the manual sub-interface configuration procedure.</td>
<td></td>
<td>Non-disruptive—Required only at edge.</td>
</tr>
<tr>
<td><strong>Shared Services</strong></td>
<td>BGP-based inter-VRF route leaking.</td>
<td>EVN-based inter-VRF route replication.</td>
<td>BGP-based inter-VRF route leaking.</td>
</tr>
<tr>
<td><strong>VN Expansion</strong></td>
<td>Limited scale. Can evolve to MPLS.</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td><strong>Layer 2 VPN Extension</strong></td>
<td>Not supported by VRF-Lite/EVN.</td>
<td></td>
<td>Supported</td>
</tr>
<tr>
<td><strong>Virtualization over WAN</strong></td>
<td>Heterogeneous with VRF enabled GRE, DMVPN.</td>
<td></td>
<td>MLS, MPLSoGRE</td>
</tr>
</tbody>
</table>
TrustSec Software Defined Microsegmentation
Policy and Microsegmentation with TrustSec

Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers.

Retaining initial VLAN/Subnet Design
TrustSec in Action

Scalable-Group Tag eXchange Protocol (SXP) – Tag Propagation
http://www.ietf.org/id/draft-smith-kandula-sxp-04.txt
Cisco TrustSec
Identity-Based Software Defined Segmentation

Desired Policy
- Who can talk to whom?
- Who can access protected assets?
- How systems can talk to other systems?

Simplified Access Management
Accelerated Security Operations
Consistent Policy Anywhere

Flexible and Scalable Policy Enforcement

<table>
<thead>
<tr>
<th>Source</th>
<th>Production Servers</th>
<th>Development Servers</th>
<th>Internet Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee (managed asset)</td>
<td>PERMIT</td>
<td>DENY</td>
<td>PERMIT</td>
</tr>
<tr>
<td>Employee (Registered BYOD)</td>
<td>PERMIT</td>
<td>DENY</td>
<td>PERMIT</td>
</tr>
<tr>
<td>Employee (Unknown BYOD)</td>
<td>DENY</td>
<td>DENY</td>
<td>PERMIT</td>
</tr>
<tr>
<td>ENG VDI System</td>
<td>DENY</td>
<td>PERMIT</td>
<td>PERMIT</td>
</tr>
</tbody>
</table>
Segmentation begins with visibility

Who is on the network?

You can’t protect what you can’t see
Visibility through NetFlow

NetFlow provides
• Trace of every conversation in your network
• An ability to collect record everywhere in your network (switch, router, or firewall)
• Network usage measurement
• An ability to find north-south as well as east-west communication
• Light weight visibility compared to SPAN based traffic analysis
• Indications of Compromise (IOC)
• Security Group Information
Visibility with Context and Control

Clear understanding of traffic flow with context

Easier to create & apply policy based on such context
Netflow Visibility Vendors: Host Locking your Network

Host groups and map to monitor network infrastructure
Modeling Policy in Netflow Visibility Vendor

Create flow-based rules for all proposed policy elements

Policy Violation alarm will trigger if condition is met. Simulating proposed drop.
Future of Network Segmentation
Future of Network Segmentation

- **Software Defined Networks (SDN)** using a Controller to simplify provisioning, policy enforcement, monitoring and troubleshooting
- Using existing Data Center protocols and technologies and moving them to the enterprise network
Further Reading

Secure Network Design: Micro Segmentation: SANS Institute
InfoSec Reading Room, Author: Brandon Peterson, Feb 2016
https://www.sans.org/reading-room/whitepapers/bestprac/secure-network-design-micro-segmentation-36775

Network Segmentation and Segregation, Australian Signals Directorate, Sept 2012

Segmenting for security: Five steps to protect your network: Network World, Nov 2014
http://www.networkworld.com/article/2851677/security0/segmenting-for-security-five-steps-to-protect-your-network.html