Managing Network Segmentation in Payment Environments

Andrew Sierra – Merchant Risk
Ed Verdurmen – Data Security Policy
Lester Chan – Merchant Security

July 22, 2015

Forward-Looking Statements

The materials, presentations and discussions during this meeting contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “will,” new,” "continue," "could," “accelerate,” and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our plans and goals regarding authentication, risk and fraud, the effect of developments in regulatory environment, and other developments in electronic payments.

By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following:

- the impact of regulation, including its effect on issuer and retailer practices and product categories, and the adoption of similar and related laws and regulations elsewhere;
- developments in current or future disputes
- macroeconomic and industry factors such as: global economic, political, health and other conditions; competitive pressure on customer pricing and in the payments industry generally; material changes in our customers' performance compared to our estimates; and disintermediation from the payments value stream through government actions or bilateral agreements;
- systemic developments, such as: disruption of our transaction processing systems or the inability to process transactions efficiently; account data breaches involving card data stored by us or third parties; increased fraudulent and other illegal activity involving our cards; failure to maintain interoperability between our and Visa Europe's authorization and clearing and settlement systems; loss of organizational effectiveness or key employees; and
- the other factors discussed under the heading "Risk Factors" herein and in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q.

You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

Notice of Disclaimer

The information, recommendations or “best practices” contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance.

Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

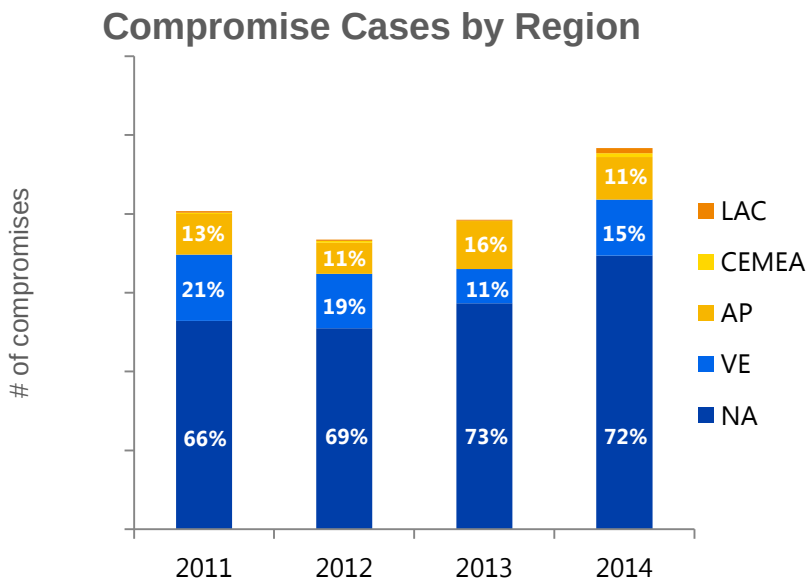
Agenda

- Global Data Compromises
- Cyber Threats and Attacks
- Payment Card Attack Example
- Today's Network Concerns and Challenges
- Network Segmentation in PCI DSS
- Segmentation and Flat Network Risks
- Securing the Network Perimeter
- Examples of Network Segmentation
- Zero Trust Principle
- Key Takeaways

Global Data Compromises

Andrew Sierra – Merchant Risk

Global Data Compromises



- Global data compromise events grew 23% in 2014 over those managed in 2013
- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- VE and AP represent the next largest contributors to known breach events, together compromising a quarter of the total
- Breaches in VE and AP are primarily CNP (93% for VE; 94% for AP)

Data Compromises

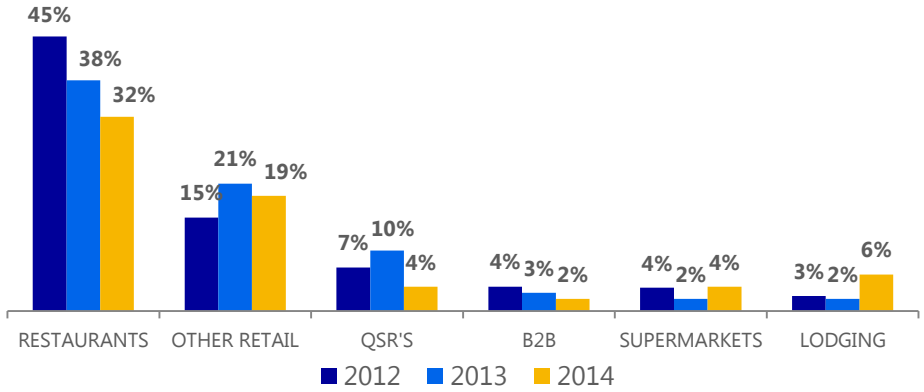
Breach trends by merchant level and Merchant Category Code

Breach Events by Merchant Level

Entity Type		2012	2013	2014
		%	%	%
Merchant	Level 1	<1%	1%	1%
	Level 2	<1%	1%	1%
	Level 3	1%	4%	4%
	Level 4	95%	92%	93%
Agent		<1%	1%	1%
Other		2%	<1%	0%
Total		**100%**	**100%**	**100%**

- While level 4 (small) merchants account for the largest number of known breach events (93% in 2014), the largest impact comes from Level 1 (large) merchant breaches
- Approximately, 77% of at risk accounts in 2014 were tied back to L1 merchants

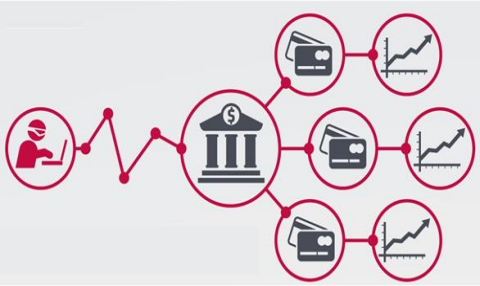
Percent of Breach Events by MCC

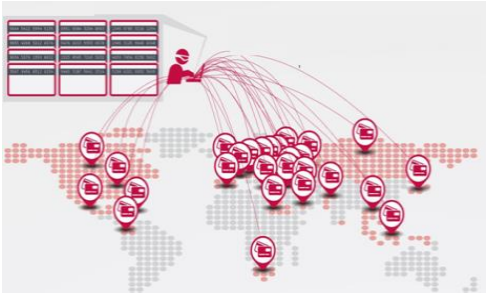


- Restaurants and “other retail” make up the biggest portion of total known breaches (32% and 19%, respectively, in 2014)
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs
- High-volume restaurants and retailers continue to be at risk

Data Compromises

Common breach patterns





Entry

- Hackers targeting internet-exposed remote access systems as initial intrusion points
- Once in, attackers conduct network reconnaissance using diagnostic tools/techniques to identify systems with access to payment data and isolate specific user accounts
- They create custom attack scripts and tools inside the merchant's network to further extend access

Card Data Theft

- Payment card data is extracted with specialized, difficult to detect malware
- Malware is named to appear as legitimate security software, in some cases
- Card data is encrypted to avoid detection
- In many recent instances, traces of attacker activity are removed, including self-deleting malware

Monetization

- Payment data is used to commit fraud, often across countries via coordinated criminal activity
  - ATMs
  - Gift cards
  - High-value goods
- Cards carry a typical value of between $20-$50 on markets for stolen data

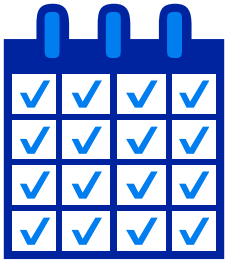
Note: There may be a significant lag between a breach and monetization

Cyber Threats and Attacks

Ed Verdurmen – Data Security and Third Party Risk

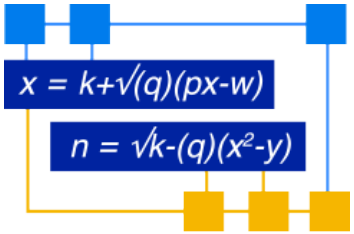
Trends in Data Compromises

Criminals are launching more sophisticated attacks

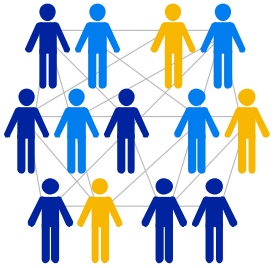


FREQUENCY

MAGNITUDE

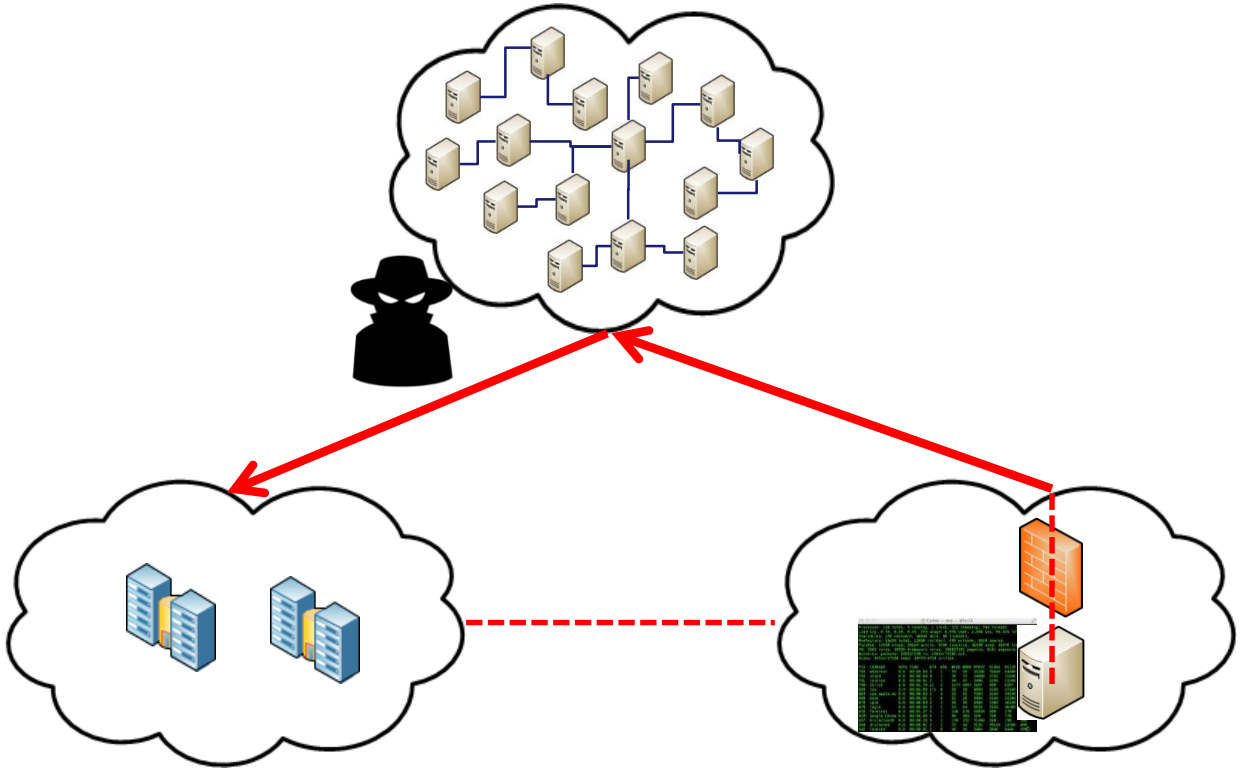


SOPHISTICATION



ORGANIZATION

Remote Access Brute Force Attack

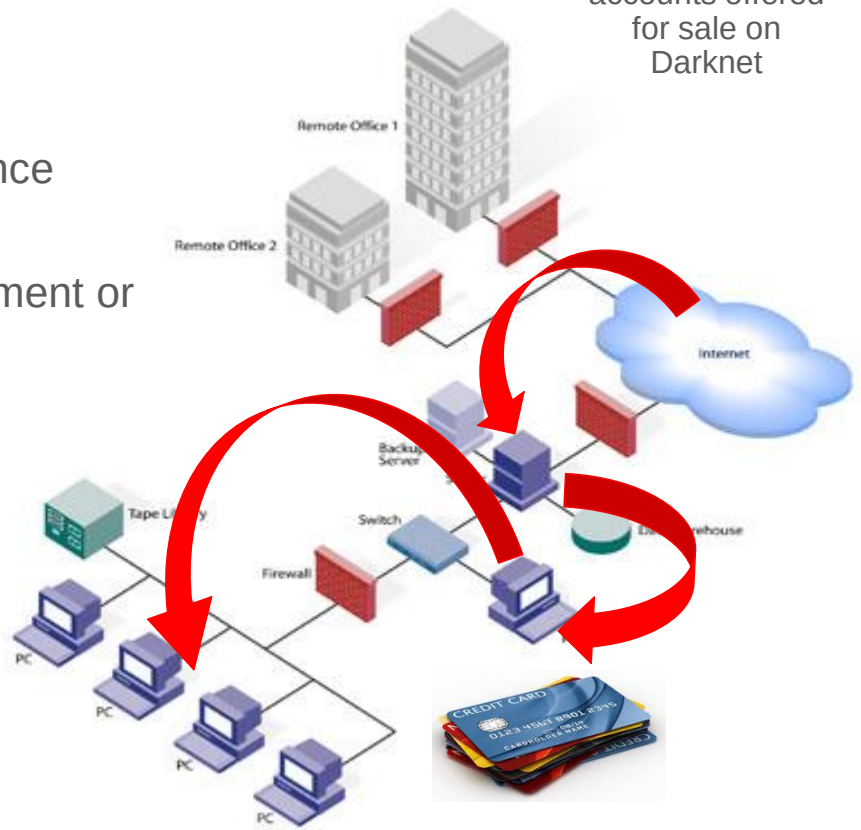


Payment Card Attack

Attacker will pivot and elevate privileges

1. Attacker steals remote login credentials
2. Attacker performs network reconnaissance
3. Attacker pivots and elevates privileges
4. Attacker gains access to patch management or software distribution server
5. Attacker distributes POS malware
6. Attacker harvests payment card data
7. Attacker exfiltrates payment card data

Payment cards accounts offered for sale on Darknet



Network Segmentation Challenges and Recommendations

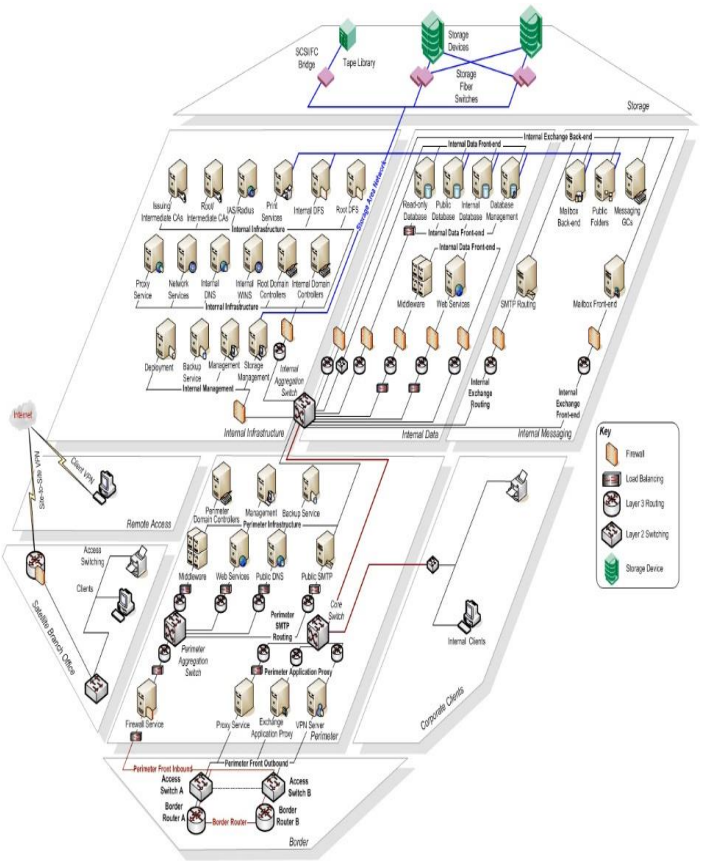
Lester Chan – Merchant Security

CISSP, CISA, CISM

Challenges with Today's Computer Networks

Complex networks make securing them difficult

- Reliability and scalability are top network concerns
- Wireless, DMZ, datacenter, extranet/intranet, BYOD
- Focused on speed, bandwidth, availability
- Most networks do not have security in mind
- Identity management and access management
- Multiple (sometimes insecure) protocols
- Grant access to authorized users
  - While keeping unauthorized users out



Network Segmentation in PCI DSS

Requirement versus Recommendations

- According to the PCI DSS*:
  - Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:
    - The scope of the PCI DSS assessment
    - The cost of the PCI DSS assessment
    - The cost and difficulty of implementing and maintaining PCI DSS controls
    - The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

* PCI DSS Version 3.1: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Introduction to Network Segmentation

Flat network risks

- Method of separating environment systems that store, process, or transmit cardholder data from those that don't
- Network segmentation is just one security control
- Once an attacker gains access to the network, can easily access the CDE
- Without network segmentation:
  - Entire network is in scope
  - Increased risks and costs to securing network
  - Vulnerability scans* and penetration tests must be performed**
  - Expand audit logging for all components not just CDE
  - Lack of redundancy and fault tolerance, prone to failure
  - Lack of scalability and speed, higher potential for collisions
- Flat networks are a single point of failure

* PCI DSS version 3.1 Requirement 11.2 ** PCI DSS version 3.1 Requirement 11.3

Securing the Network Perimeter

Four steps to securing the network perimeter

1. **Enable secure remote access** – Always use multi-factor authentication
2. **Harden devices, update software and review policies** – Review configurations and ACLs
3. **Build layers of security** – Use defense-in-depth and next gen firewalls with content filtering, advance malware detection, IPS/IDS, identity management, and WAF
4. **Create and segment** – Use firewalls, proxies, and rules to segregate the DMZ from internal and externals users

- Be aware of remote login protocols and manage closely
  - Remote access software, port 3389

Examples of Network Segmentation Controls

From Flat Networks to Best Practices

-lat Network

- No subnetting
- Single domain
- No VLANs
- CDE located with core network

Low (Good)

- Understand network data flows
- CDE is separated by VLANs
- Use of access control lists
- Basic firewall rules

Medium (Better)

- Firewalls separate CDE from core network
- Firewall rules are reviewed audited regularly
- Granular control on users, assets, and traffic

High (Best)

- Separate login domain for CDE than core network
- Air gapped/ Completely segregated
- Alerts are regularly reviewed
- Two-factor authentication to log into CDE domain

Improving Security with Proper Segmentation

Practices and Principles

- **Cardholder Data Environment** – Ensure properly scoped and segmented
- **Manage ingress/egress to CDE** – only allow specific subnet and restrict protocols
  - Why allow port 80 (HTTP) or 21 (FTP) outbound from the CDE?
  - DENY from ANY to ANY for ANY
- **Whitelist or hybrid approach** – Instead of blocking or denying all threats, only allow permitted protocols and communication
- **Principle of least privilege** – Provide the lowest access and rights only to do their job
- **Software-Defined Networking** – Ability to perform micro-segmentation and analyze traffic across stacks or layers
- **Zero Trust Principle** – Rethinking the traditional network trust

Introduction to the Zero Trust Principle

Next Generation Secure Network

- Proposed by Forrester Research
- Embed security into network DNA
- Design from the inside out
- Design with compliance in mind
- Inspect and log all traffic
- Zero Trust – “Verify and never trust”

Traditional Model

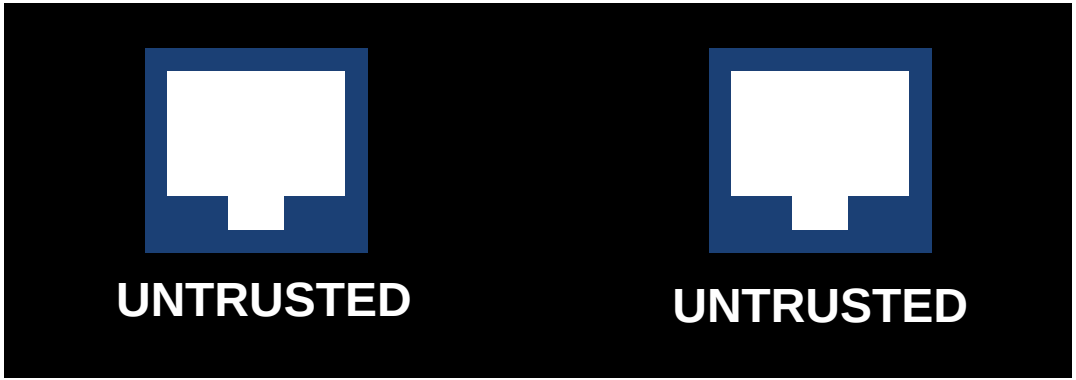
Zero Trust Model

VERIFY AND
NEVER TRUST

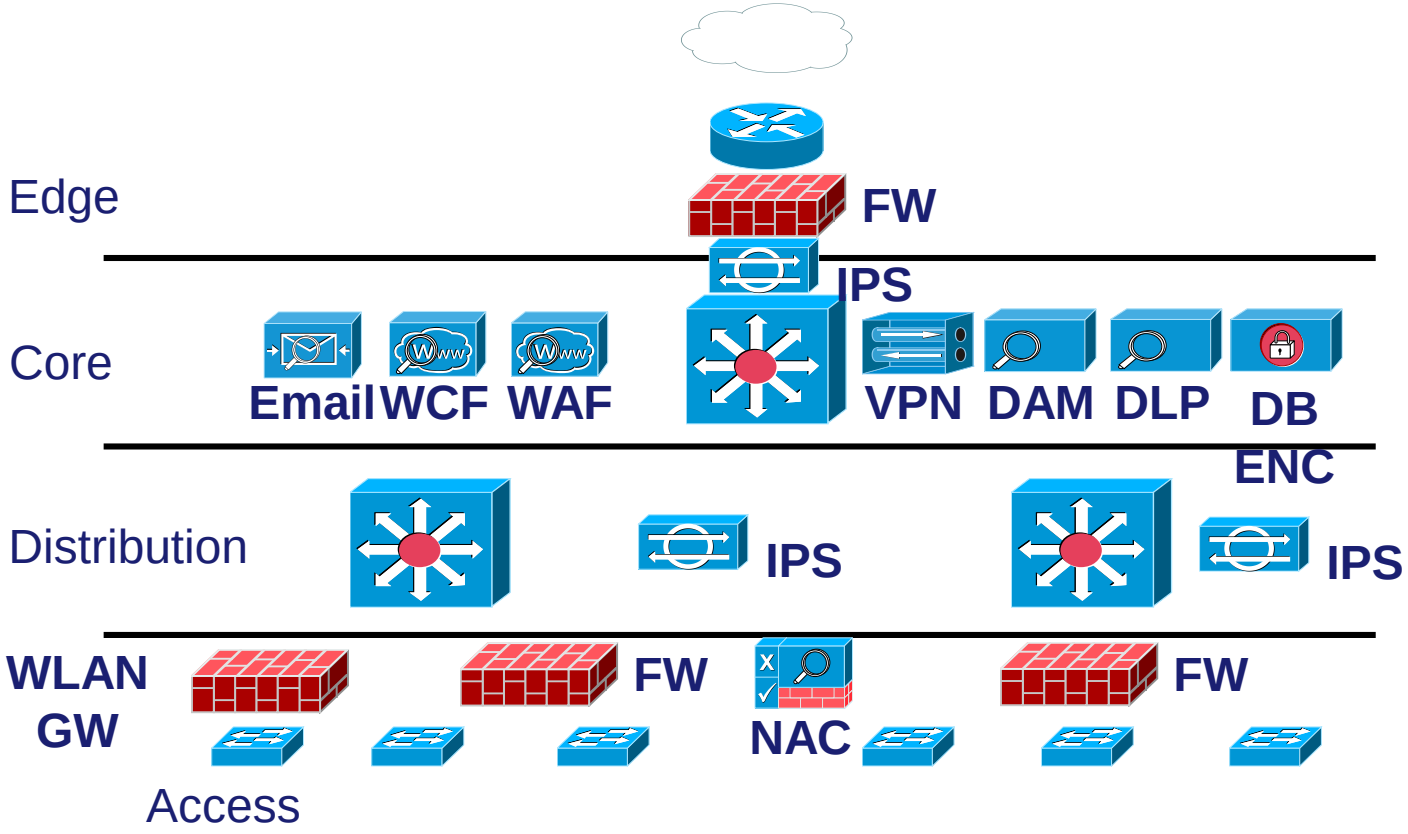
Which one goes to the Internet?

Traditional Network Trust Model

Zero Trust Model



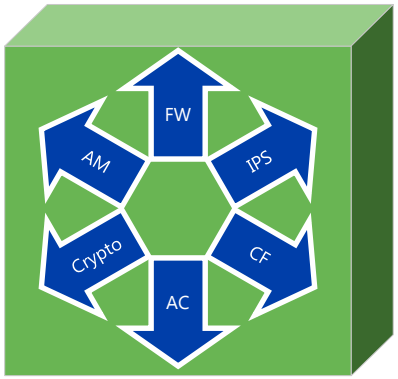
Security Is An Overlay

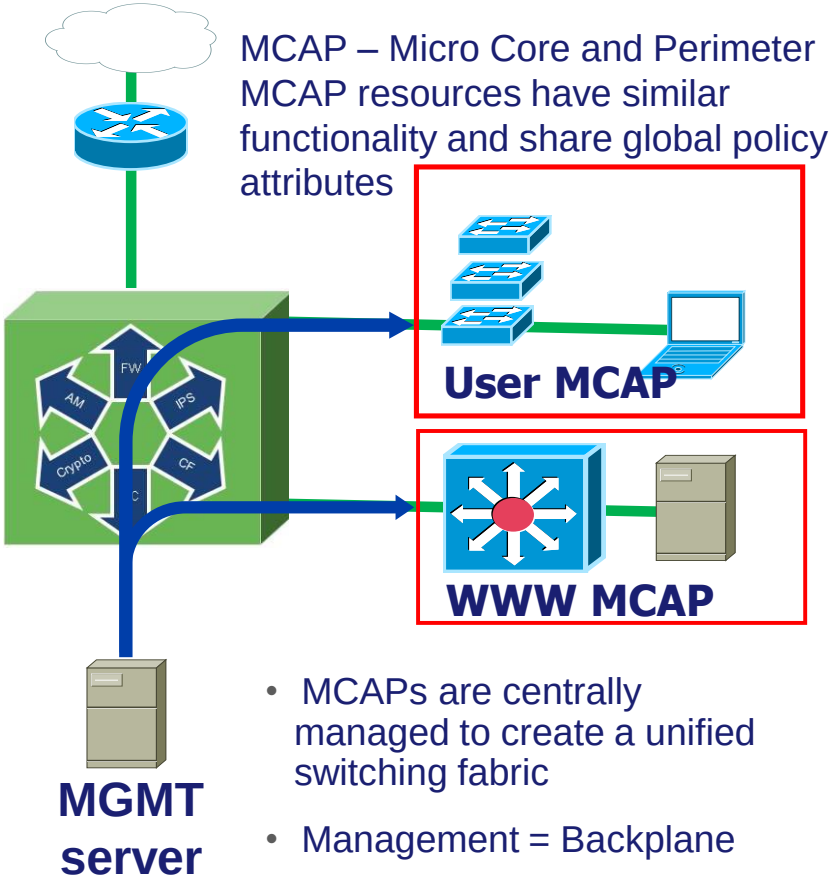


Zero Trust Drives Future Network Design

Segmentation Gateway

- NGFW
- Very High Speed
- Multiple 10G Interfaces
- Builds Security into the Network DNA





MCAP – Micro Core and Perimeter
MCAP resources have similar functionality and share global policy attributes

- MCAPs are centrally managed to create a unified switching fabric
- Management = Backplane

Key Takeaways

Lessons Learned

1. **Understand your network data flows** – Internet ingress and egress, data flows in and out of the CDE, protocols, users and services
2. **At minimum, implement ACLs and VLAN properly** – Avoid flat networks and review ACLs and policies to make it difficult for an attacker to pivot and traverse
3. **Harden the network perimeter** – Ensure the perimeter is hardened with two-factor authentication, remote access is restricted and regularly reviewed
4. **Regularly review and respond to alerts** – Ensure admins regularly review and respond to alerts to logs, SIEM, and potential attacks
5. **Consider the Zero Trust principle** – Verify and never trust, harden the core with next generation firewalls, IDS/IPS, anti-spam, APT protection
6. **Conduct regular policy audits** – Avoid set it and forget policies, conduct regular policy audits to check rules and policy

Visa is hosting a must-attend event that will focus on trends and developments related to cyber security, mobile payments, e-commerce and Visa's global authentication strategy. In order to secure the future of commerce all stakeholders including merchants, acquirers, agents and Visa need to collaborate on key initiatives in addressing today's most relevant issues. This event will be held in the San Francisco Bay Area at the Hyatt Regency Hotel just south of San Francisco.

Upcoming Events and Resources

Upcoming Webinars – Under Merchant Resources/Training on www.visa.com

- **Payment Card Data and Protected Health Information Security Practices**, August 5,2015
- **Implementing Effective Penetration Testing**, August 25, 2015
- **The Importance of Containment and Remediation of Compromised Payment Processing Environments**, September 2, 2015

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

- Streamline your chip migration – www.VisaChip.com/businesstoolkit

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards, QIR Listing
- Fact Sheets –Mobile Payments Acceptance, Tokenization, and many more…

Thank you for attending!

Questions? Comments?