Protect and Manage Resources

- WAF, Shield, Firewall Manager
- Instance Metadata Service (V2)
- Secrets Manager
- Systems Manager
- Config
- Inspector
- Trusted Advisor

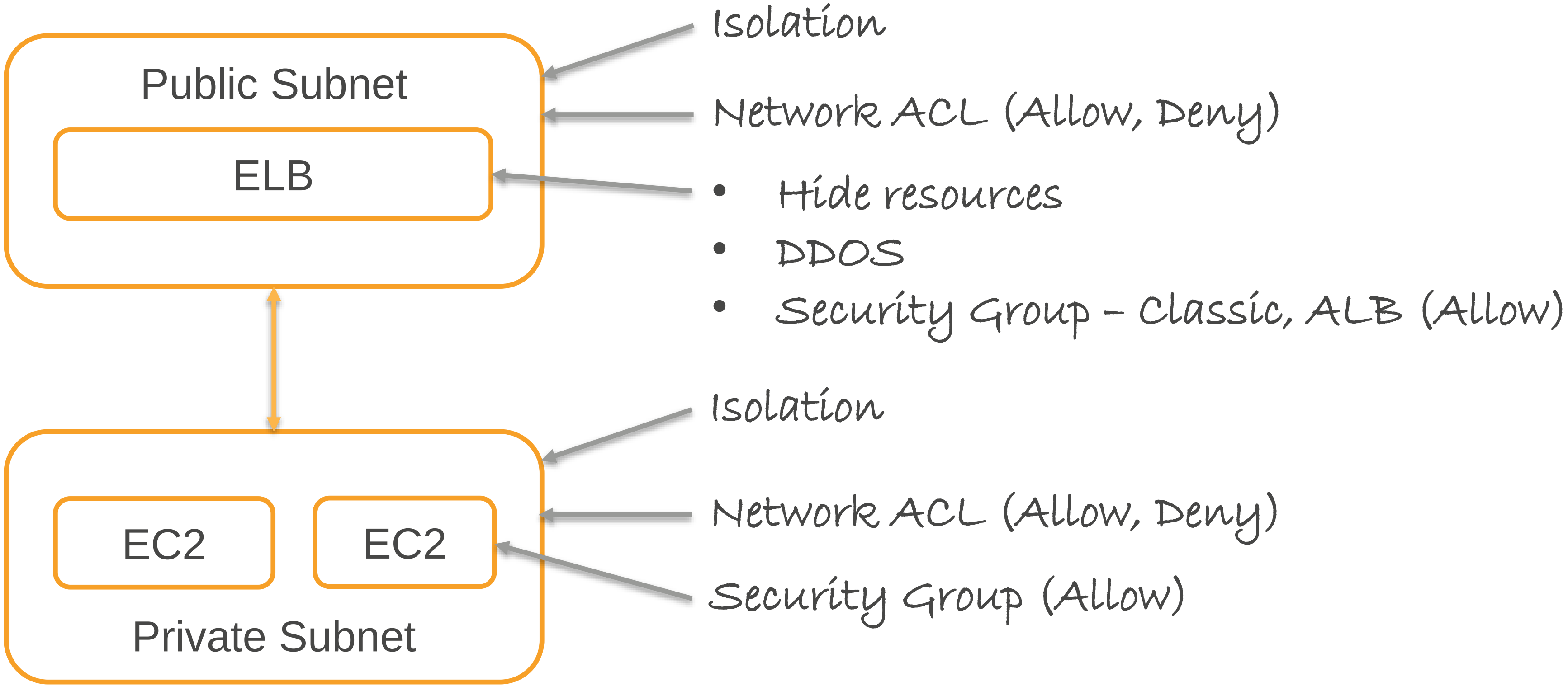
WAF, Shield

Comprehensive security solution to protect your application and infrastructure

Chandra Lingam

Cloud Wave LLC

Motivation



Public Subnet

ELB

Private Subnet

EC2

EC2

Isolation

Network ACL (Allow, Deny)

- Hide resources
- DDOS
- Security Group – Classic, ALB (Allow)

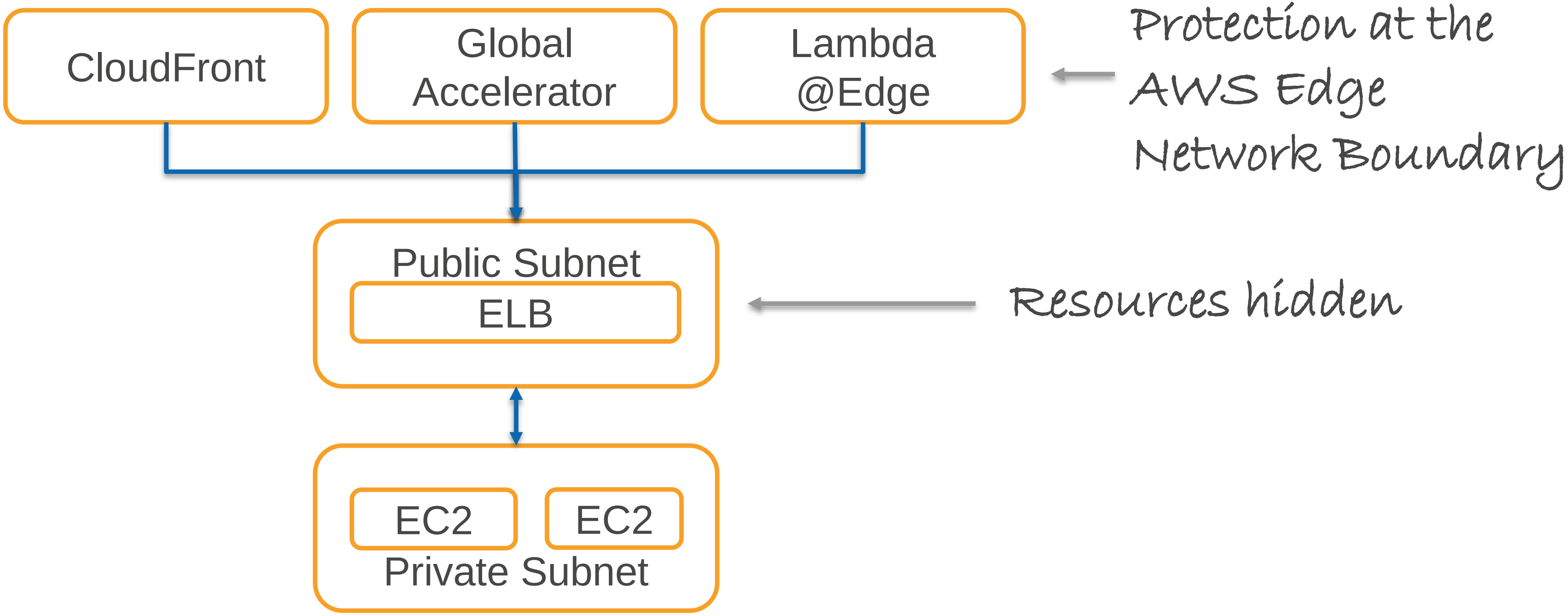
Isolation

Network ACL (Allow, Deny)

Security Group (Allow)

Essential, but does not protect against software vulnerabilities

Edge Protection



Essential, but does not protect against software vulnerabilities

Injection Attacks

http://example.com/accounts?username=alice

```
query = "SELECT * FROM accounts WHERE owner = '" + userName + “’”
```

```
"SELECT * FROM accounts WHERE owner = ‘alice’”
```

References:
OWASP Top Ten - Globally recognized by developers as the first step towards more secure coding.
https://owasp.org/www-project-top-ten/

Common Weakness Enumeration - a community-developed list of common software and hardware security weaknesses
https://cwe.mitre.org/data/definitions/89.html

Injection Attacks

```
http://example.com/accounts?username=alice’ OR ‘1’=‘1

query = "SELECT * FROM accounts WHERE owner = '" + userName + “’”

"SELECT * FROM accounts WHERE owner = ‘alice’ OR ‘1’=‘1’”
```

References:
OWASP Top 10 - Globally recognized by developers as the first step towards more secure coding.
https://owasp.org/www-project-top-ten/

Common Weakness Enumeration - a community-developed list of common software and hardware security weaknesses
https://cwe.mitre.org/data/definitions/89.html

Server-Side Request Forgery

What We Can Learn from the Capital One Hack

“On Monday, a former Amazon employee was arrested and charged with stealing more than 100 million consumer applications for credit from Capital One.”

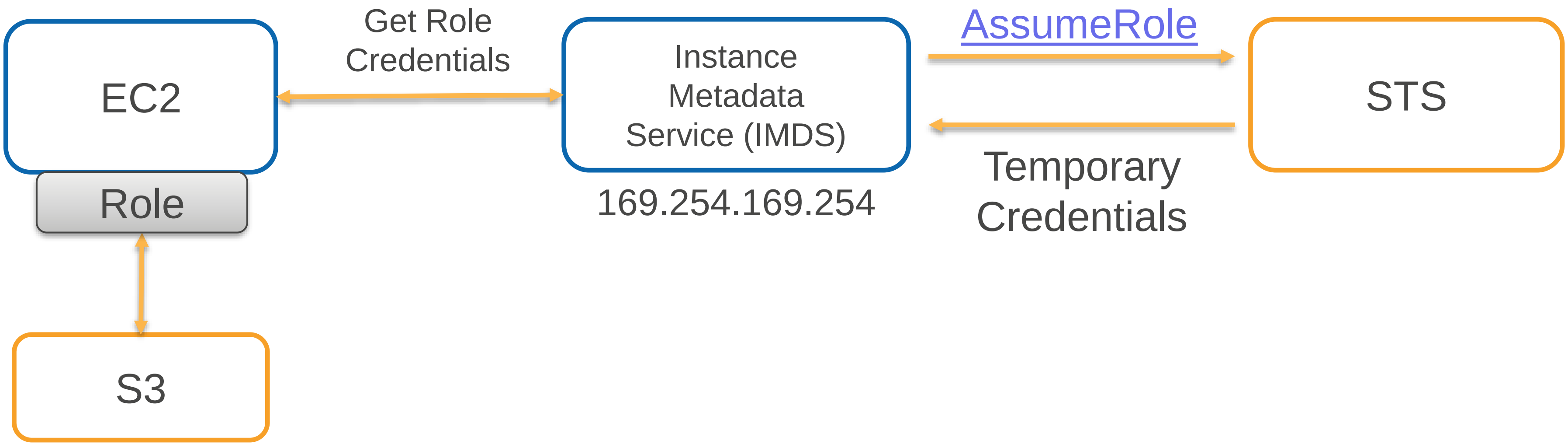
“That data included approximately 140,000 Social Security numbers and approximately 80,000 bank account numbers on U.S. consumers, and roughly 1 million Social Insurance Numbers (SINs) for Canadian credit card customers.”

Source:

https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/

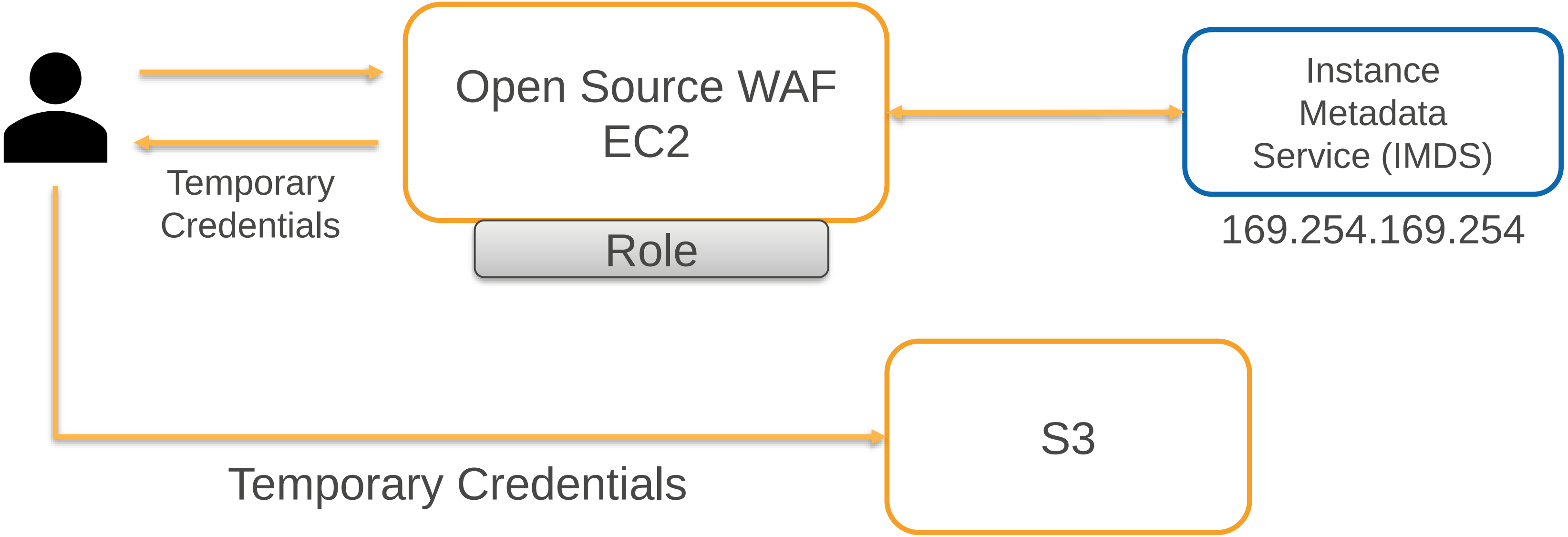
EC2 Instance Metadata Service (IMDS-V1)



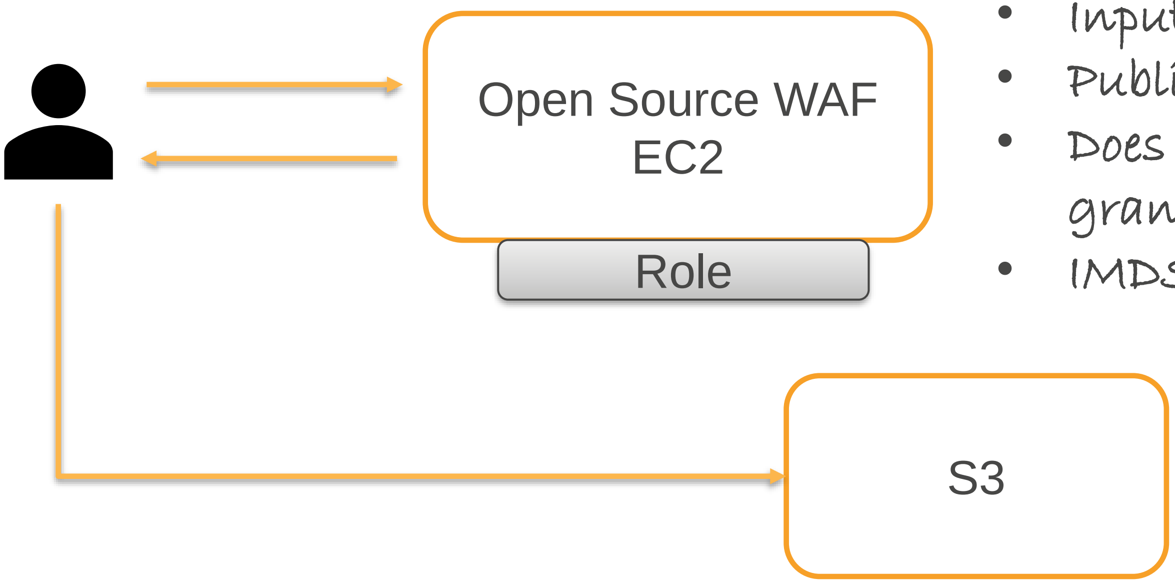
Metadata service call to retrieve temporary security credentials for IAM Role
http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name

SSRF Attack

http://example.com/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name



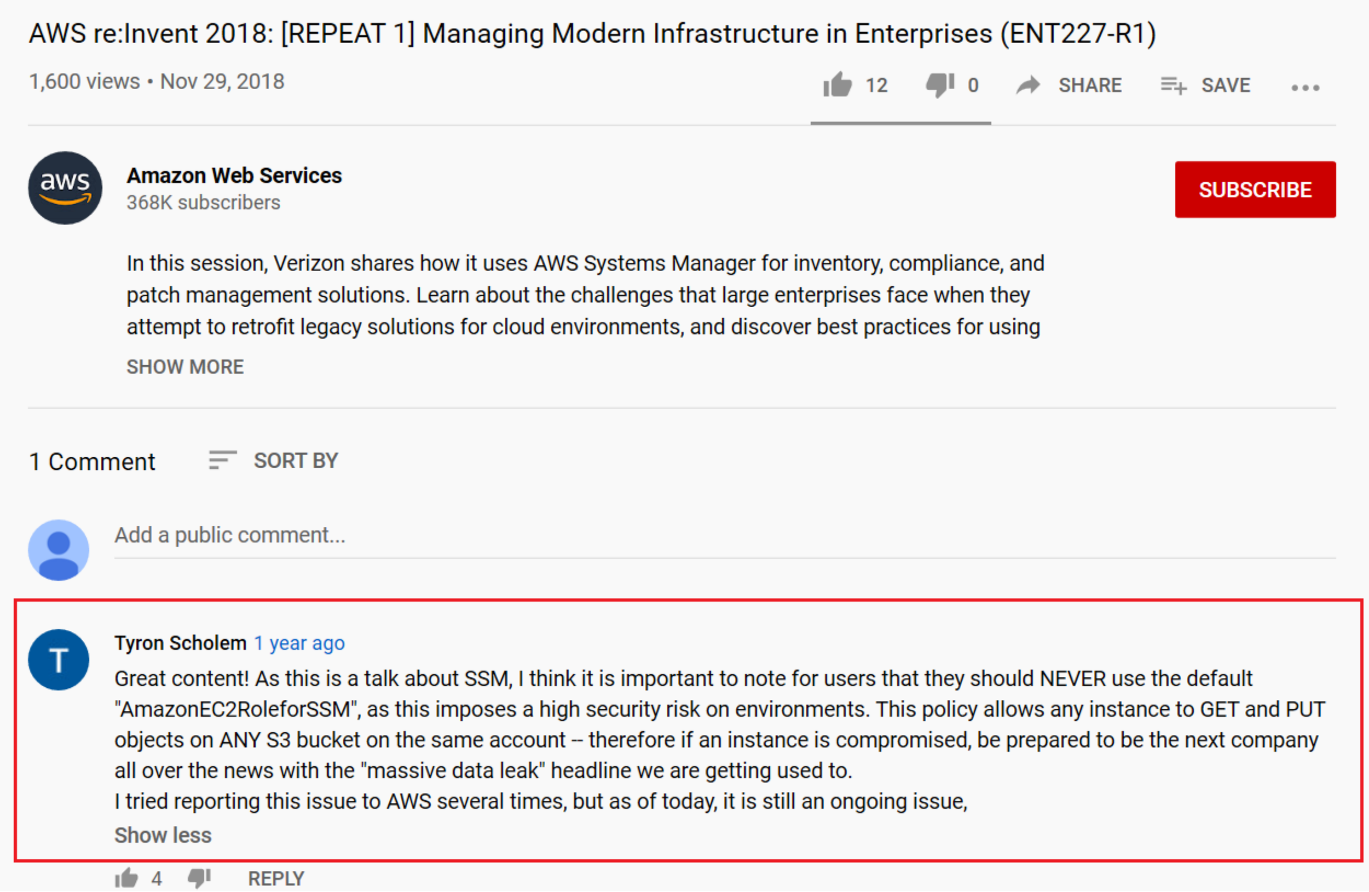
SSRF Attack – how to fix this?



- Input Validation
- Public or Intranet
- Does it need an IAM Role or grant least privilege
- IMDS V2

- SSE-KMS Encryption
- Deny access that are not from corporate network or VPC
- Tag based permissions

AWS EC2 Systems Manager



AWS re:Invent 2018: [REPEAT 1] Managing Modern Infrastructure in Enterprises (ENT227-R1)

1,600 views • Nov 29, 2018

Amazon Web Services
368K subscribers

In this session, Verizon shares how it uses AWS Systems Manager for inventory, compliance, and patch management solutions. Learn about the challenges that large enterprises face when they attempt to retrofit legacy solutions for cloud environments, and discover best practices for using

1 Comment

Add a public comment...

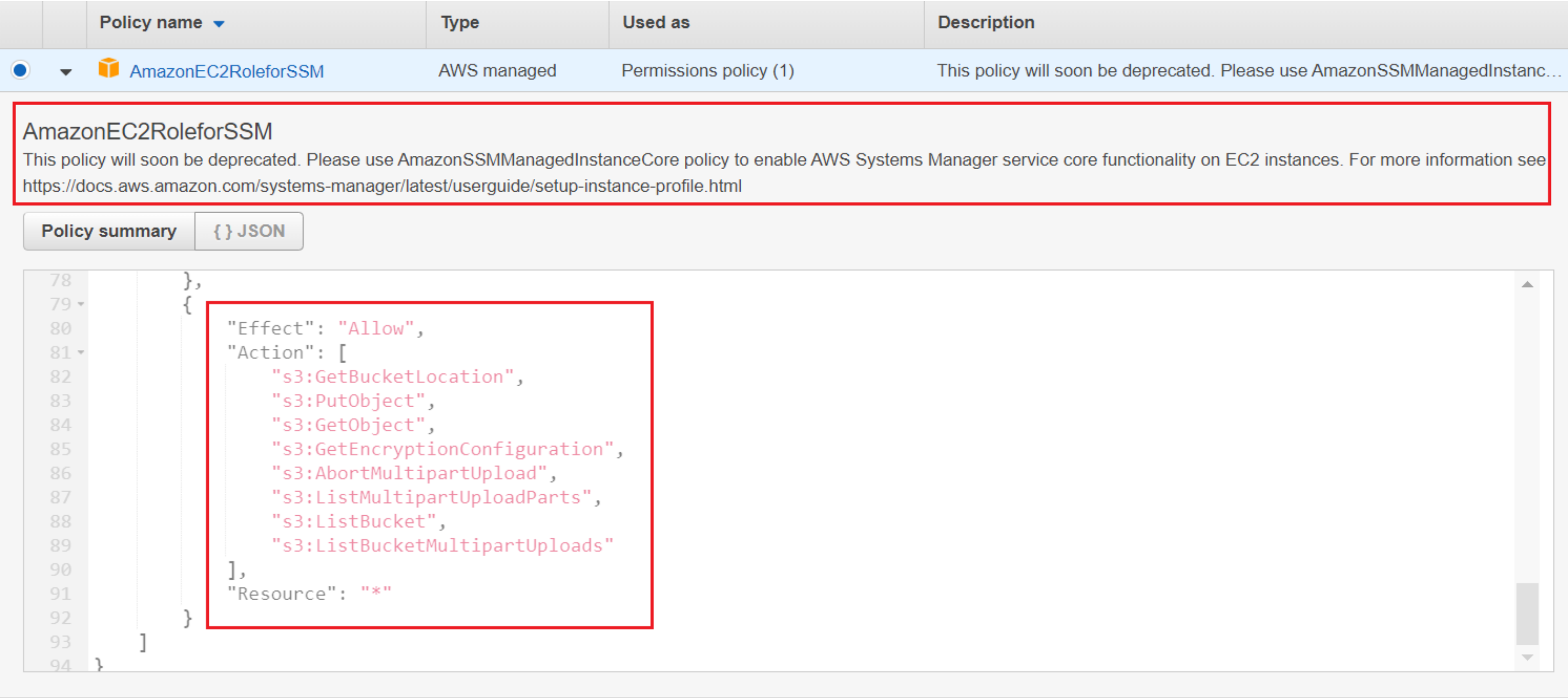
Tyron Scholem 1 year ago

Great content! As this is a talk about SSM, I think it is important to note for users that they should NEVER use the default "AmazonEC2RoleforSSM", as this imposes a high security risk on environments. This policy allows any instance to GET and PUT objects on ANY S3 bucket on the same account -- therefore if an instance is compromised, be prepared to be the next company all over the news with the "massive data leak" headline we are getting used to.
I tried reporting this issue to AWS several times, but as of today, it is still an ongoing issue,

AWS Systems Manager

AmazonEC2RoleforSSM - Grants access to all S3 buckets

AmazonSSMManagedInstanceCore – Safer replacement



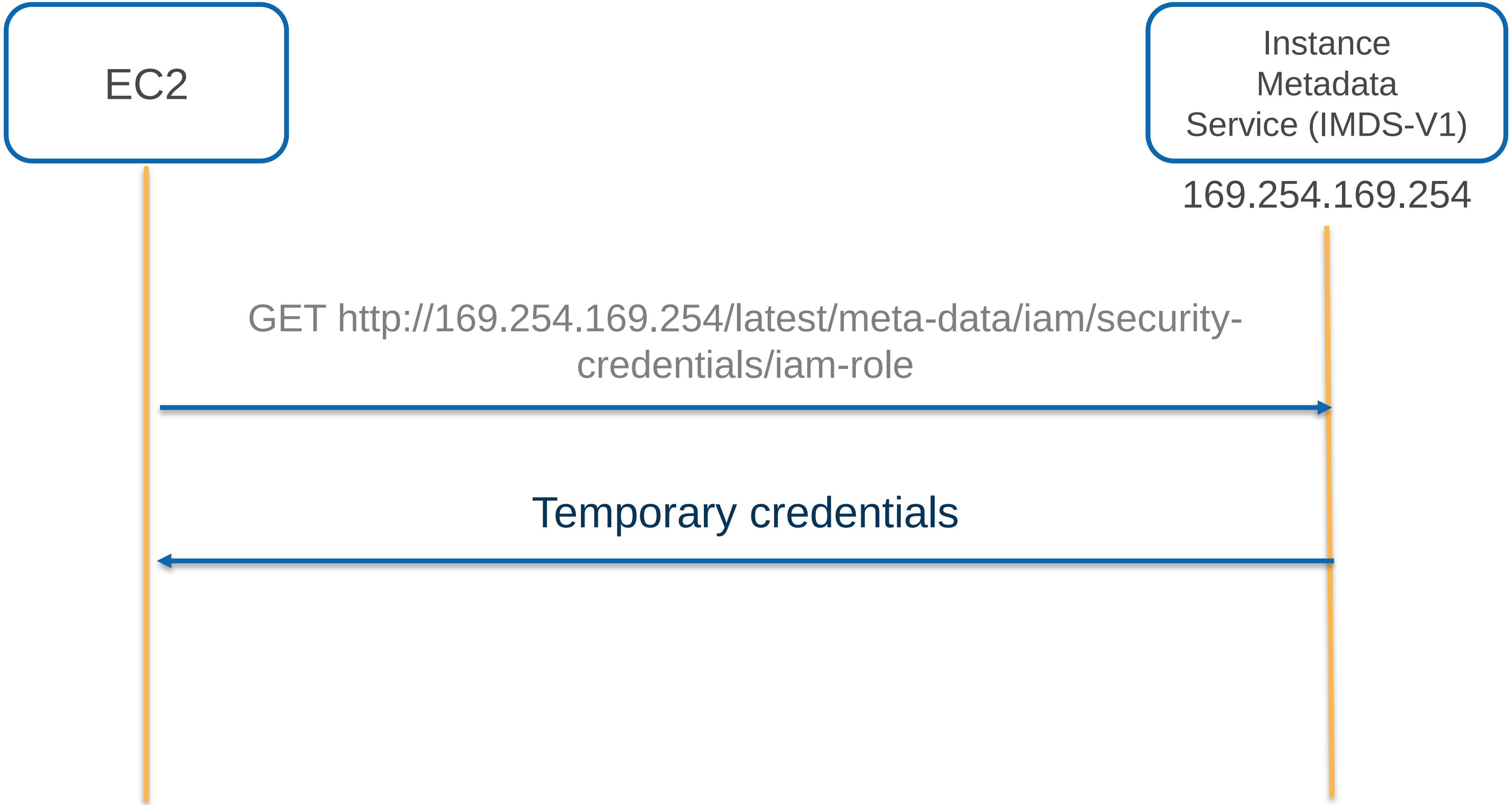
		Policy name ▼	Type	Used as	Description
●	▼	AmazonEC2RoleforSSM	AWS managed	Permissions policy (1)	This policy will soon be deprecated. Please use AmazonSSMManagedInstanc…

AmazonEC2RoleforSSM

This policy will soon be deprecated. Please use AmazonSSMManagedInstanceCore policy to enable AWS Systems Manager service core functionality on EC2 instances. For more information see https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "*"
        }
    ]
}
```

EC2 IMDS (V1)



EC2

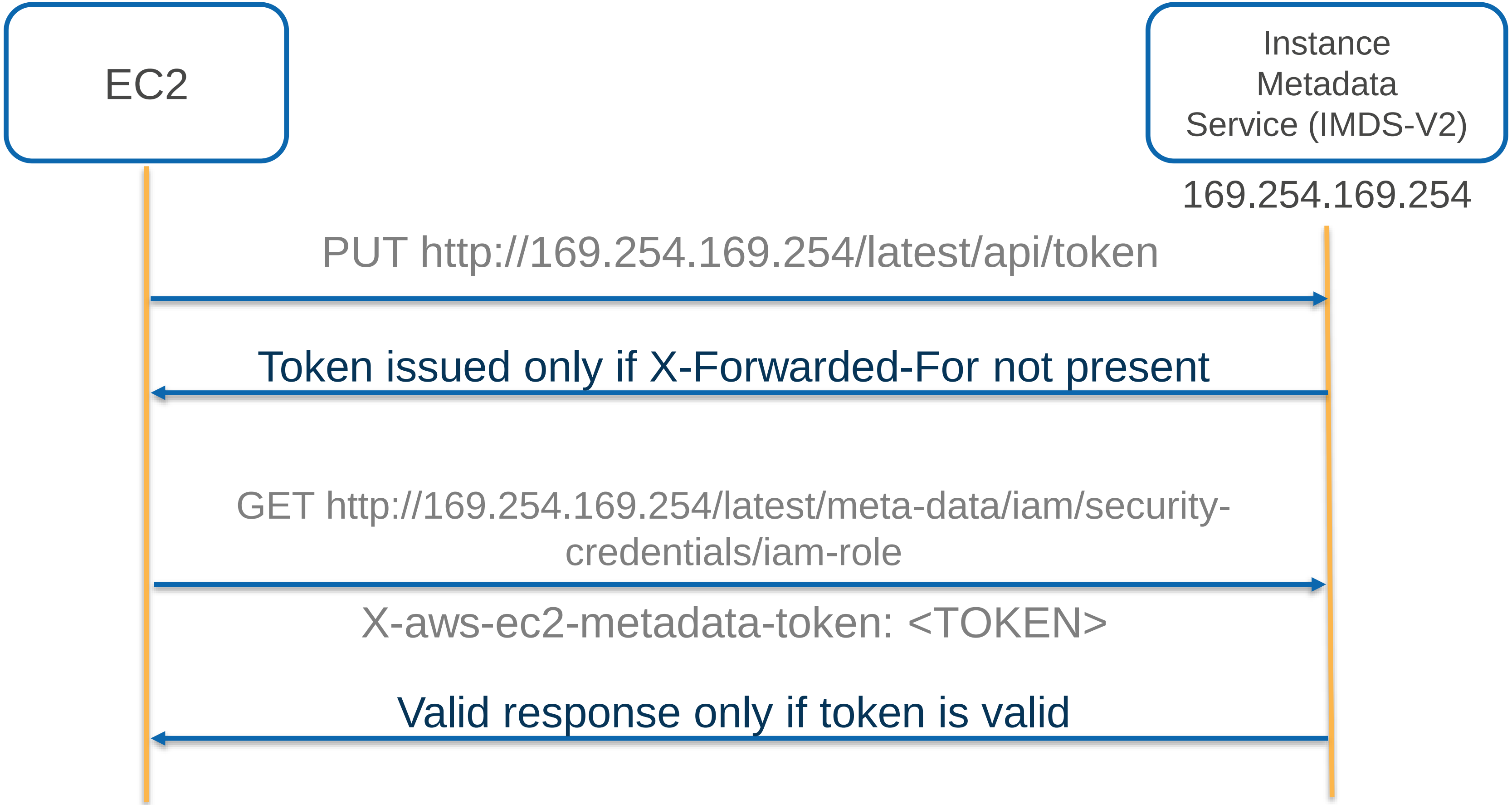
Instance Metadata Service (IMDS-V1)

169.254.169.254

GET http://169.254.169.254/latest/meta-data/iam/security-credentials/iam-role

Temporary credentials

EC2 IMDS (V2)



EC2

Instance Metadata Service (IMDS-V2)

169.254.169.254

PUT http://169.254.169.254/latest/api/token

Token issued only if X-Forwarded-For not present

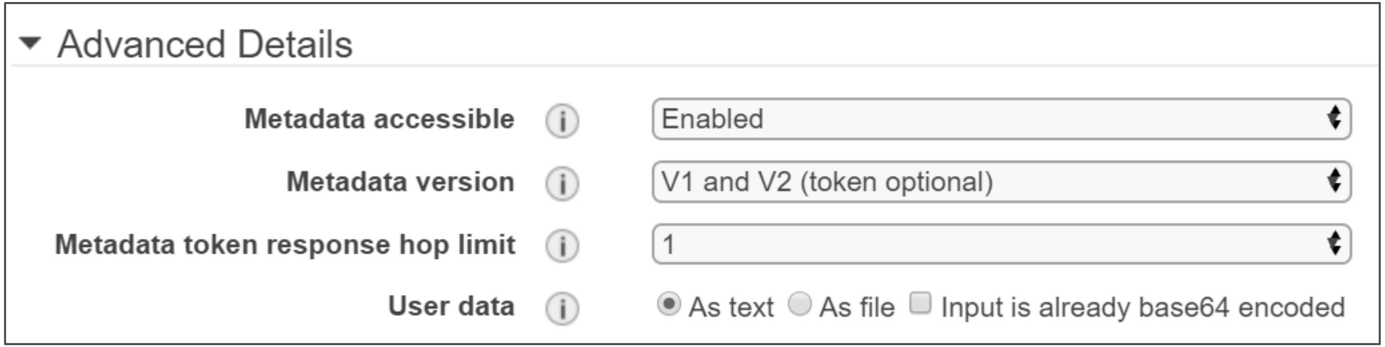
GET http://169.254.169.254/latest/meta-data/iam/security-credentials/iam-role

X-aws-ec2-metadata-token: <TOKEN>

Valid response only if token is valid

EC2 IMDS (2020)

IMDS Mode	Purpose
Metadata accessible	Enabled – Instance can query metadata service Disabled - Metadata service endpoint is disabled
Metadata Version	V1 and V2 (token optional) V2 (token required)



▾ Advanced Details

Metadata accessible	Enabled
Metadata version	V1 and V2 (token optional)
Metadata token response hop limit	1
User data	● As text ○ As file □ Input is already base64 encoded

Lab – EC2 IMDS V2 Demo

- Launch EC2 instance in IMDS V1 and V2 mode
- Metadata service accessible with or without token

- Enable V2 mode
- Metadata service not accessible without token

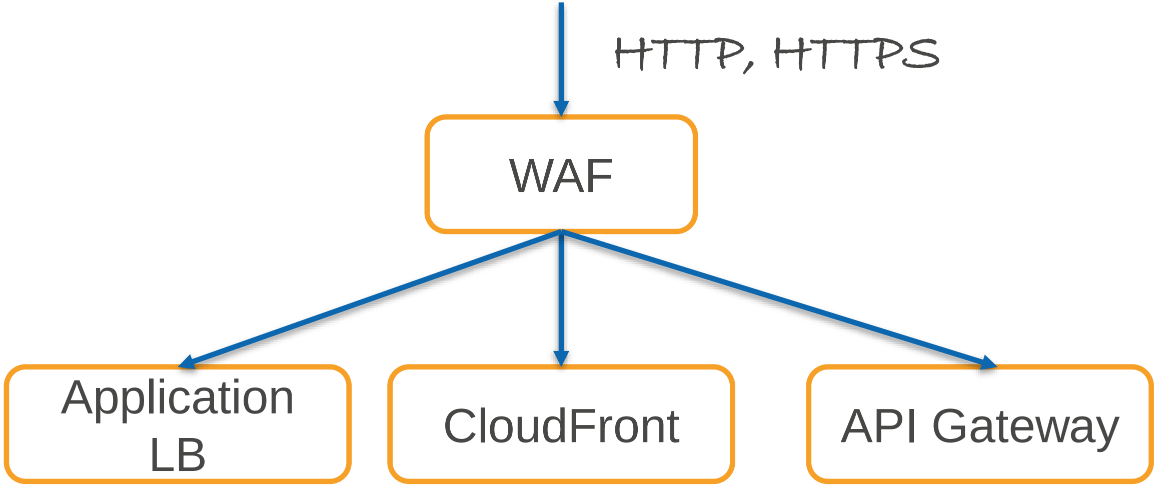
AWS Products

Service	Purpose
AWS Web Application Firewall	Application Layer Protection (Layer 7)
AWS Shield – Standard	• Infrastructure Layer Protection (Layer 3, 4) • Included for all customers (Free)
AWS Shield – Advanced	• DDoS Response Team (business and enterprise support plans) • Metrics, Alarms, Reports (visibility into attack) • Protection against regional and global resources • Includes WAF • DDoS autoscaling Cost Protection
AWS Firewall Manager	Simplifies administration and maintenance tasks across multiple accounts (WAF rules, Shield Advanced, VPC Security Groups)

Application Layer Attacks (Layer 7)

- OWASP Top 10 – Top 10 most critical risks to web applications
  - Injection
  - Broken Authentication
  - Sensitive Data Exposure
  - XML External Entities
  - Broken Access Control
  - Security misconfiguration
  - Cross-site Scripting
  - Insecure Deserialization
  - Using Components with known vulnerabilities
  - Insufficient Logging and Monitoring
- HTTP Flood
- Cache-busting attacks

AWS WAF – Protection from common exploits



- Protect your web application from common exploits
- Monitor requests to Application Load Balancer, CloudFront, API Gateway (and more)
- Secure at the edge (with CloudFront, CloudFront query parameter whitelist)
- Visibility with CloudWatch Metrics, Comprehensive logging

Web Access Control List (ACL)

Container of rules and rule groups

Rules define criteria for inspecting the web request and how to handle requests that match the criteria

Rule groups are collection of rules and they are reusable

Associate Web ACL with one or more resources (CloudFront, ALB, API Gateway, and more)

Rule changes are propagated in under one minute

WAF – Managed Rule Groups

Preconfigured set of rules managed by AWS and Marketplace Sellers

- OWASP Top 10
- Common Vulnerabilities and Exposure (CVE)
- AWS IP Reputation List – Block addresses associated with bots and other threats
- AWS IP Anonymous List – Block requests from services that obfuscate caller identity (VPN, Proxies, Tor nodes)

Automatically updated for new threats

Lab – WAF protection on ALB

ALB with a single webserver

Define WAF ACL

Add AWS managed rule groups to block common exploits

Protect ALB using WAF

Rule Action

Action	Purpose
Block	Blacklisting. Deny based on content or condition Example: • Block all OWASP 10 vulnerabilities, • Block requests based on IP reputation, • Rate limit - block requests that exceed specified count during a 5-minute window (temporary)
Allow	Whitelisting. Allow based on content or condition Example: • Allow based on readily identifiable information, • Limit access to users from specific countries
Count	Count the requests that match the properties you specify Example: • Observe the traffic, • Refine the rules

Rules can inspect a request based on

- IP Address Sets (greater limit than Security Groups – 100s of thousands vs ~300)
- Country
- Values in request header
- Strings that appear in the request
- Regex pattern Sets
- Length of request
- Presence of SQL Code
- Presence of script

WAF Pricing

- USD 5.00 per web ACL per month (prorated hourly)
- USD 1.00 per rule per month (prorated hourly)
- USD 0.60 per million request processed
- Managed Rules are priced by the seller
- Cost effective

AWS Shield

AWS Shield Standard

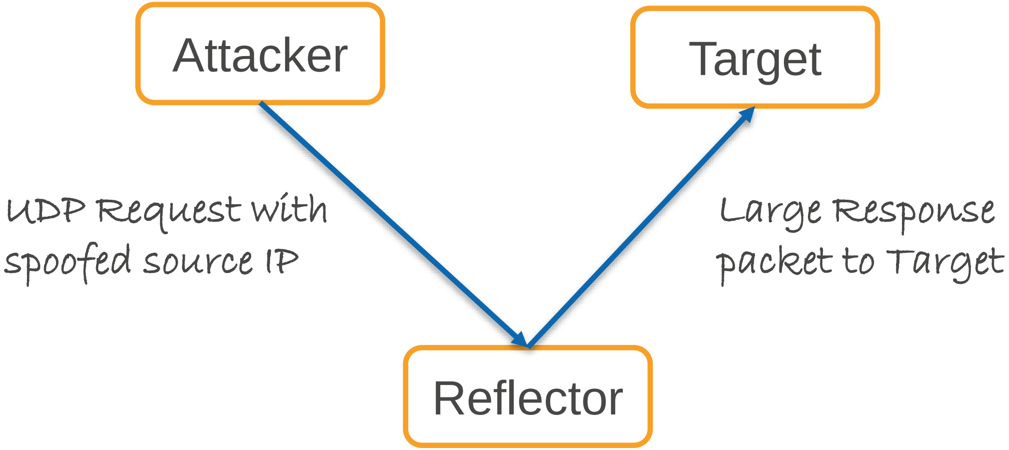
Protection against Layer 3 and 4 attacks

DDoS and other infrastructure level attacks

Included for all customers

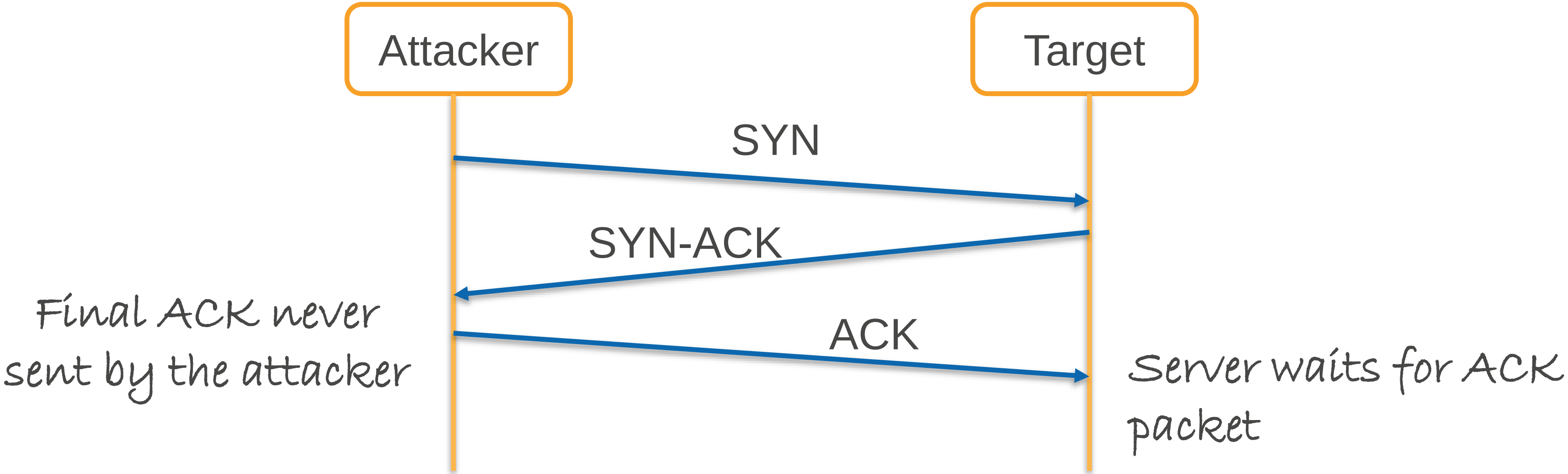
Free

UDP reflection attack (Layer 3)


Attacker
Target
UDP Request with spoofed source IP
Large Response packet to Target
Reflector

Reference: AWS Best Practices for DDoS Resiliency

SYN Flood (Layer 4)


Attacker
Target
SYN
SYN-ACK
ACK
Final ACK never sent by the attacker
Server waits for ACK packet

Reference: AWS Best Practices for DDoS Resiliency

AWS Shield Advanced

DDoS Response Team (with business and enterprise support plan)

Visibility and Reporting

CloudWatch metrics to alert you of attacks

Includes WAF

AWS Shield Advanced Protection

- Individual EC2 instances, ELBs, Elastic IPs
- CloudFront distributions
- Route 53 hosted zones
- Global Accelerators

AWS Shield Advanced Pricing

- Fixed charges - USD 3,000 per month for an organization (covers all accounts that are part of an organization)
- Data transfer out
- Includes WAF
- Cost Protection against scaling events due to DDoS

Additional Resources

Best Practices for DDoS Mitigation on AWS

https://www.youtube.com/watch?v=HnoZS5jj7pk

Whitepaper: AWS Best Practices for DDoS Resiliency

AWS Products

Service	Purpose
AWS Web Application Firewall	Application Layer Protection (Layer 7)
AWS Shield – Standard	Infrastructure Layer Protection (Layer 3, 4) Included for all customers (Free)
AWS Shield – Advanced	DDoS Response Team (business and enterprise support plans) Visibility into attack Protection against regional and global resources Includes WAF DDoS autoscaling Cost Protection
AWS Firewall Manager	Simplifies administration and maintenance tasks across multiple accounts (WAF rules, Shield Advanced, VPC Security Groups)

Manage Resources at Scale

- Secrets Manager
- Systems Manager
- Config
- Inspector
- Trusted Advisor

1000s of resources to manage

- Users
- S3 Buckets
- VPC
- Security Groups
- Network ACL
- EC2 Instances
- EBS Volumes
- Load Balancers
- Containers

Million ways to mis-configure

ACCESS KEY ROTATION

SOFTWARE INVENTORY

DATABASE BACKUP

Automated and Continuous Monitoring to manage resources at scale

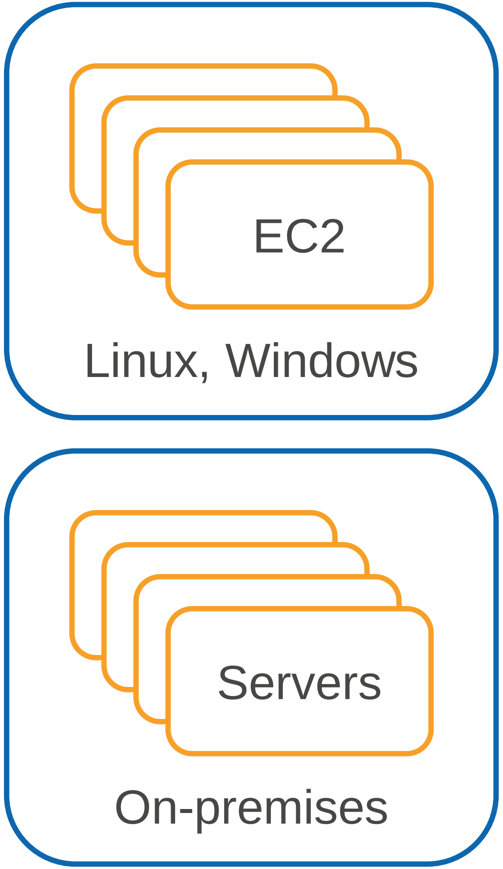
AWS Secrets Manager

Secrets

- Database credentials
- Passwords
- SSH Keys
- API Keys
- OAuth Tokens

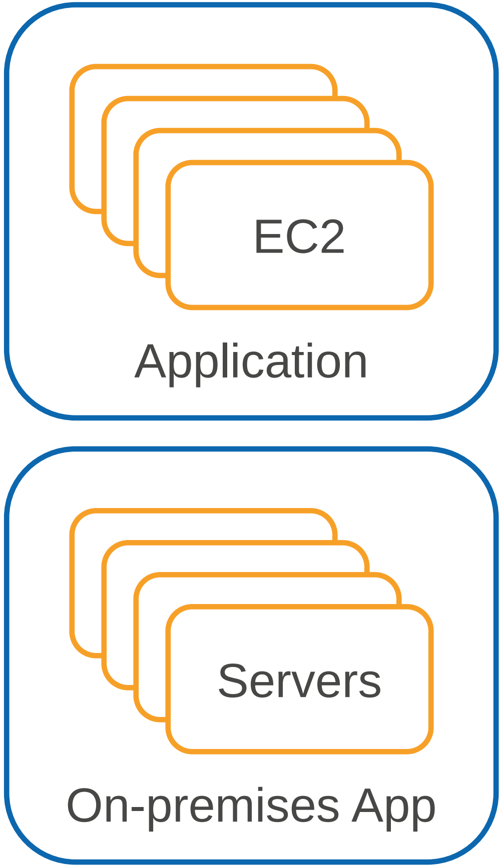
- Encrypt with KMS
- Control access using IAM
- Tag-based access control
- Rotate credentials
- Lambda integration for custom rotation
- Access using SDK, CLI
- CloudFormation
- Audit and Monitor usage
- USD 0.40 per secret per month
- USD 0.05 per 10,000 calls

AWS Systems Manager



- Patch Management
- Run Commands across a fleet of instances
- Session Manager - Interactive shell/CLI for Linux and Windows
- IAM based access to servers
- No need for SSH/RDP/Bastion Host
- Inventory – OS, Software, Configuration (AWS Config integration)
- Parameter Store – Configuration data and secrets

AWS Systems Manager



- State Manager – Maintain consistent configuration (anti-virus, firewall, server setting)
- Automation of routine administrative tasks (example: Create AMI, Recover impaired instances, stop instance with approval)
- App Config - Manage application configuration and changes

AWS Config

- Compare current and desired state of resources
- Managed ready to use rules, Create custom rules
- Change history
- Multi-account, multi-region data aggregation
- Systems Manager integration (OS, Application, System level config)
- Alert when changes detected

AWS Config – Managed Rule Checks

- Access key rotated periodically
- ALB HTTP to HTTPS redirection configured
- Unused EBS Volumes, unused Elastic IP
- Check if multi-az is configured for RDS
- Verify is S3 bucket has bucket-level encryption enabled
- Check if EC2 instance is managed by systems manager

Managed Rules: https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html

AWS Config

- ✓ Compare current and desired state of resources
- Managed ready to use rules, Create custom rules
- ⇆ Change history
- Multi-account, multi-region data aggregation
- Systems Manager integration (OS, Application, System level config)
- ⚠ Alert when changes detected

AWS Best Practices

Compare with Your Implementation

AWS Inspector

Security exposures and vulnerabilities in your EC2 instances

Network Assessment

- Ports reachable from outside the VPC
- Processes reachable on the port (with Inspector agent)

Host Assessment

- Vulnerable software (CVE)
- Host hardening (CIS Benchmarks)
- Security best practices
- Requires Inspector Agent

AWS Trusted Advisor

Scans and compares your infrastructure against AWS best practices

COST OPTIMIZATION

PERFORMANCE

SECURITY

FAULT TOLERANCE

SERVICE LIMITS

Trusted Advisor Core Checks

All Customers have access to seven core checks

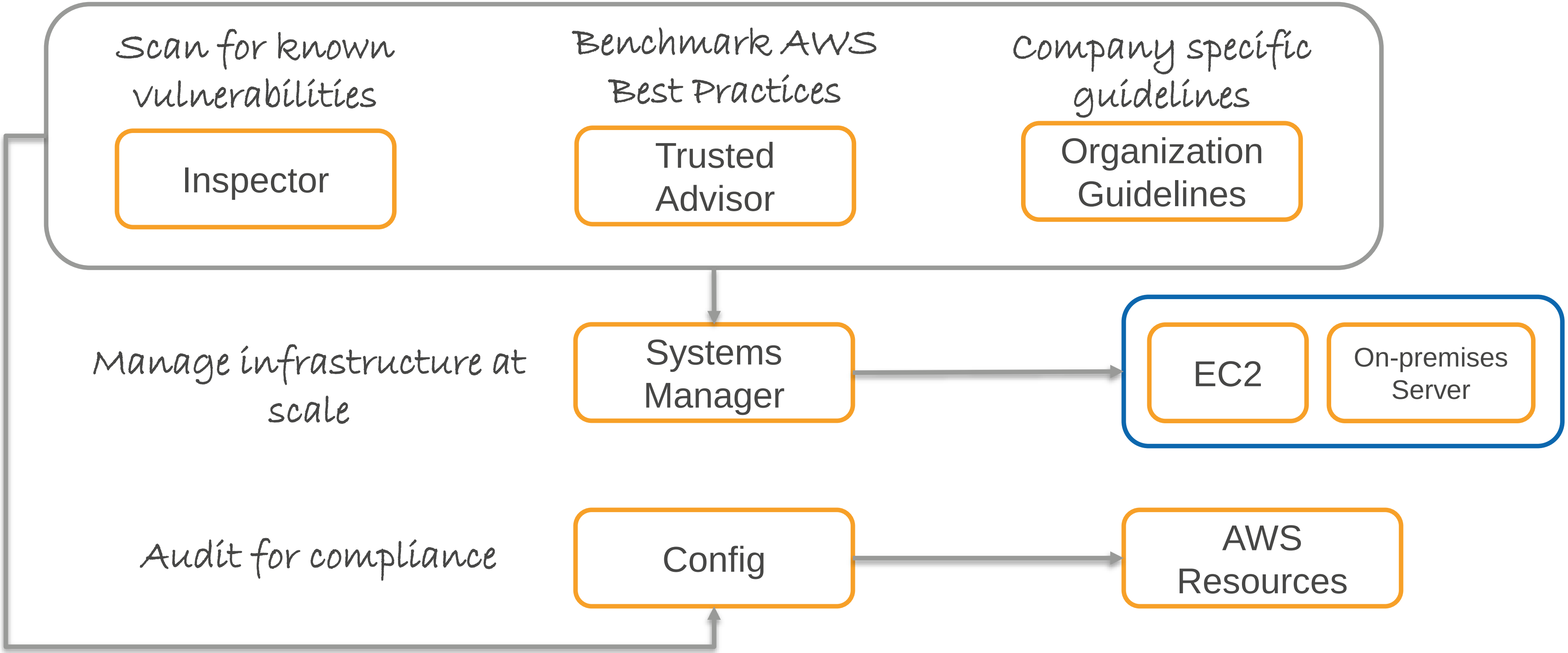
Example:

- S3 bucket permissions
- Security Groups - Specific ports that are unrestricted
- IAM use, MFA on root account
- EBS Public snapshots
- RDS Public snapshots
- Service Limits

Trusted Advisor – Full Checks

Customers with Business and Enterprise Support have access to full set of trusted advisor checks

Putting it all together



Scan for known vulnerabilities

Inspector

Benchmark AWS Best Practices

Trusted Advisor

Company specific guidelines

Organization Guidelines

Manage infrastructure at scale

Systems Manager

EC2

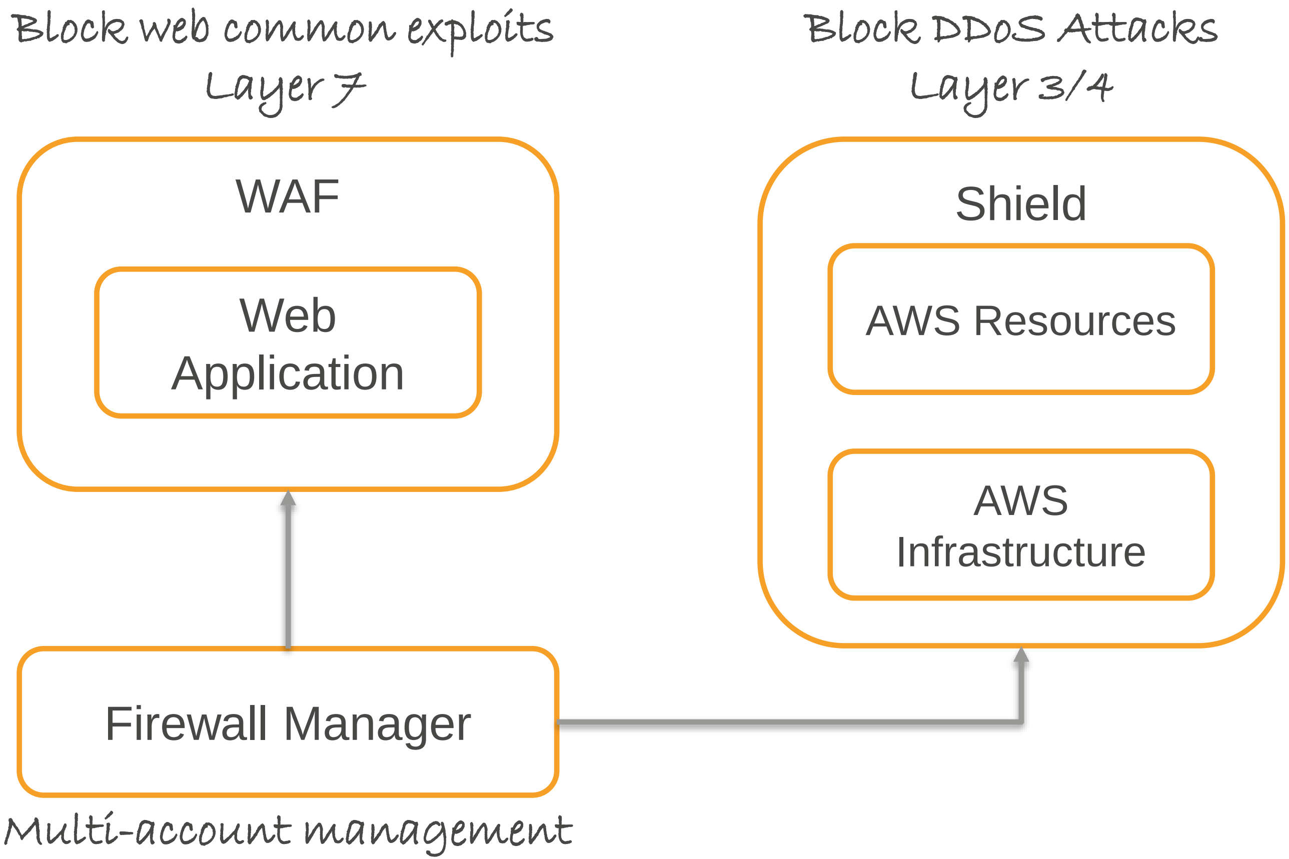
On-premises Server

Audit for compliance

Config

AWS Resources

Putting it all together



Chandra Lingam

57,000+ Students

For AWS self-paced video courses, visit:

https://www.cloudwavetraining.com/

Cloud Wave LLC