Contents

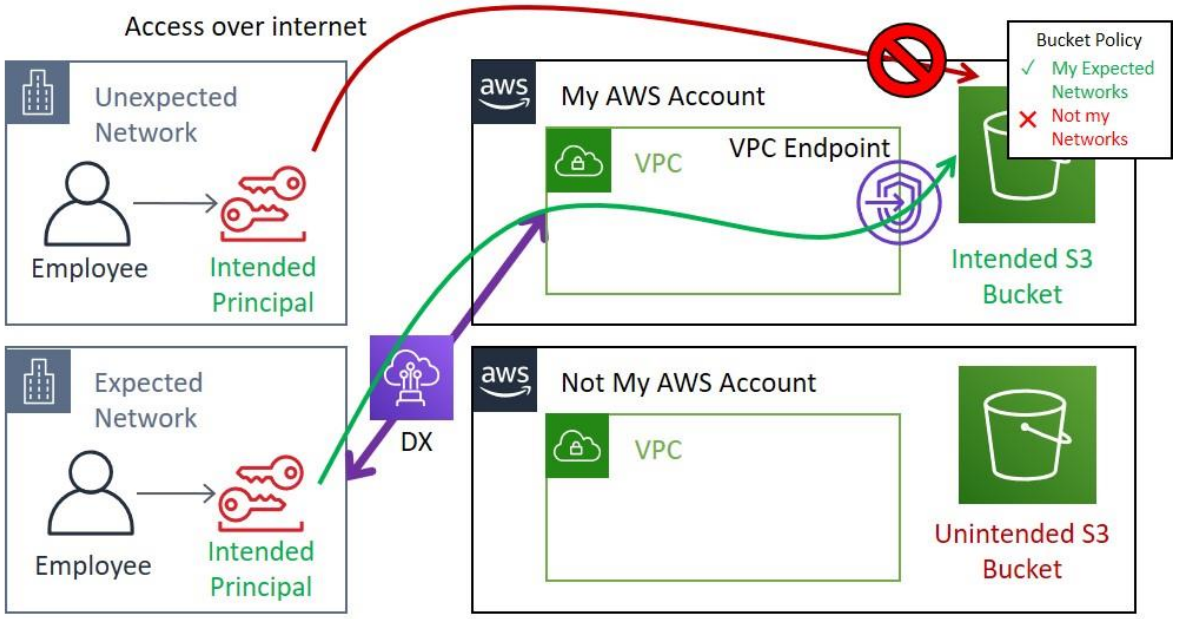

***Figure 5 - Preventing Access from Unexpected Networks**: The S3 bucket policy (a resource-based policy) prevents access from unexpected network locations.*

Network Boundary

The Network Boundary consists of VPC endpoint policies applied to VPC endpoints in expected networks (your VPCs) that ensure only intended identities (Only My IAM Principals) can access intended resources (Only My Resources) from your expected networks.

This boundary's purpose is to prevent data from moving to unintended resources outside the perimeter by unintended IAM principals whom are not subject to your IAM identity-based policies or SCPs.

VPC endpoint policies provide a mechanism to prevent actions by unintended principals in both your VPC and on-premises networks. In VPC networks, traffic is routed to VPC endpoints automatically if you are using AWS provided DNS.

For on-premises networks, you can also route AWS traffic through VPC endpoints if they are connected to AWS via AWS Direct Connect or VPN. For services that have PrivateLink interface endpoints, you can route traffic to those endpoints directly from an on-premises network. When using an Amazon DynamoDB that only provides a gateway endpoint, you can use a proxy fleet as a way to route traffic from on-premises over that endpoint. This control ensures that unintended principals can't move data outside your network perimeter to other AWS locations.

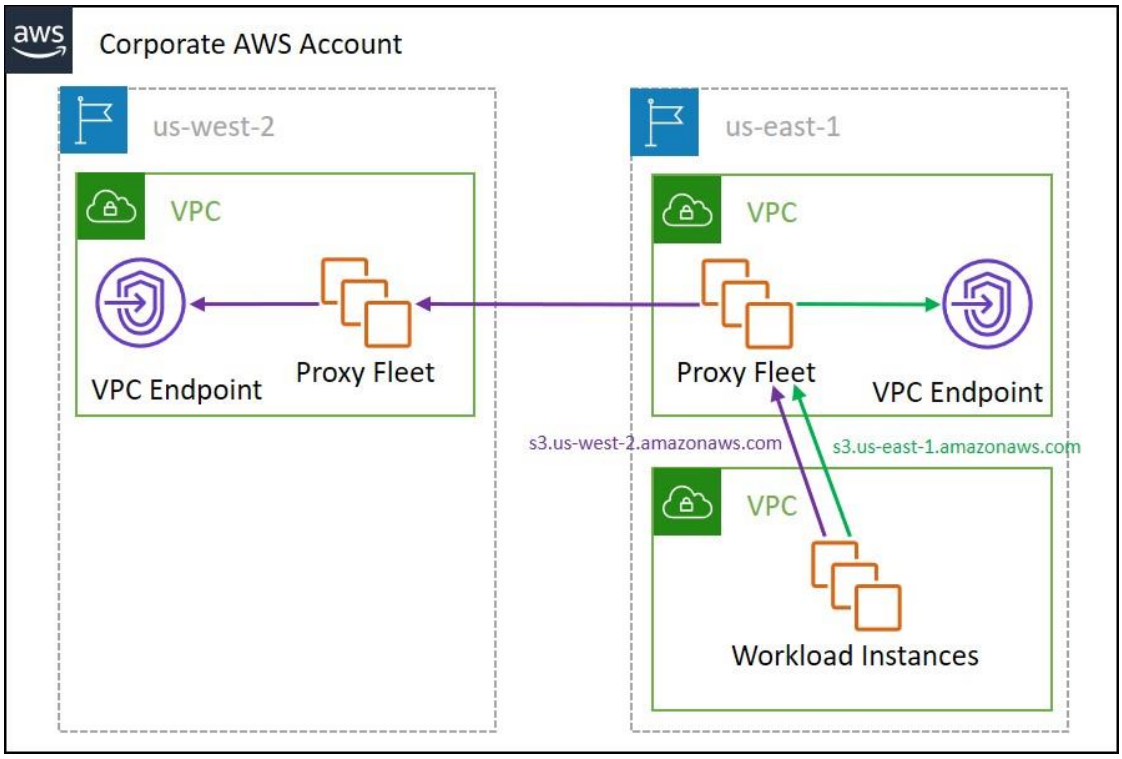

Figure 8 - Using Proxy-Chaining to Send Out-Of-Region Requests through VPC Endpoints*: Workloads send their HTTPS traffic to a proxy in the same Region. That proxy sends "in-Region" requests to the appropriate VPC endpoint and forwards "out-of-Region" requests to a peer proxy.*

Preventing Access to Temporary Credentials

Except for the cases of credential theft or leakage, the only other way for an unintended entity to gain access to temporary credentials derived from IAM roles that are part of "my AWS", is through misconfigured IAM role trust policies.

IAM role trust policies define the principals that you trust to assume an IAM role. A role trust policy is a required resource-based policy that is attached to a role in IAM. The principals that you can specify in the trust policy include users, roles, accounts, and services.

The trust policy can be configured to ensure that no one from outside the customer's account or organization can be authorized to assume the role. Customers should audit all IAM role trust policies and ensure one of the following are true.

```
cache_peer_access dub allow eu_west_1
cache_peer_access dub allow eu_west_1_alt

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

## Explicitly allow approved AWS Regions so we can block
## all other Regions using .amazonaws.com below
http_access allow rfc_1918 us_east_1
http_access allow rfc_1918 us_east_2
http_access allow rfc_1918 us_west_2
http_access allow rfc_1918 eu_west_1
http_access allow rfc_1918 us_east_1_alt
http_access allow rfc_1918 us_east_2_alt
http_access allow rfc_1918 us_west_2_alt
http_access allow rfc_1918 eu_west_1_alt

## Block all other AWS Regions
http_access deny aws_domain

## Allow all other access from local networks
http_access allow rfc_1918
http_access allow localnet

## Finally deny all other access to the proxy
http_access deny all

## Listen on 3128
http_port 3128

## Logging
access_log stdio:/var/log/squid/access.log
strip_query_terms off
logfile_rotate 1

## Turn off caching
cache deny all

## Enable the X-Forwarded-For header
forwarded_for on

## Suppress sending squid version information
httpd_suppress_version_string on
```

```
## How long to wait when shutting down squid
shutdown_lifetime 30 seconds

## Hostname
visible_hostname aws_proxy

## Prefer ipv4 over v6
dns_v4_first on
```

Contributors

Contributors to this document include:

- Michael Haken, Principal Solutions Architect, Amazon Web Services

Document Revisions

Date	Description
September 2021	Content and policy example updates
July 2021	First publication

Notes

[1] https://en.wikipedia.org/wiki/If_and_only_if