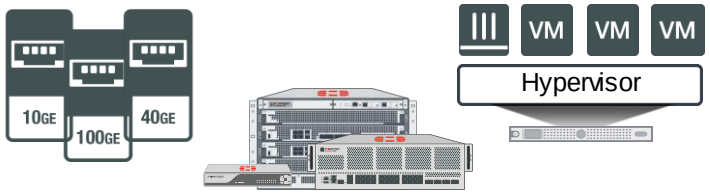
Network Security Reference Architecture

Alex Samonte – Director of Technical Architecture

Network Security Architecture Components

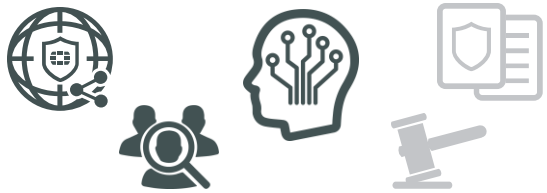
Open Ecosystem

Scalable Multi-Formfactor

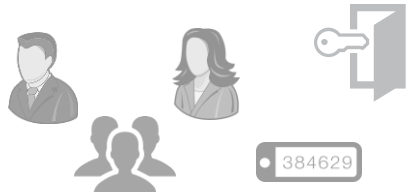


Network & Security Operations & Analytics

Security Intelligence



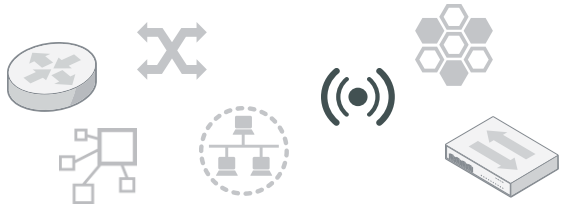
Identity & Access Management



Advanced Response

Automated Broad Integrated

Networking Flexibility



Threat Protection

Antivirus IPS ATP Anti-Spam Anti-Botnet

Content Visibility

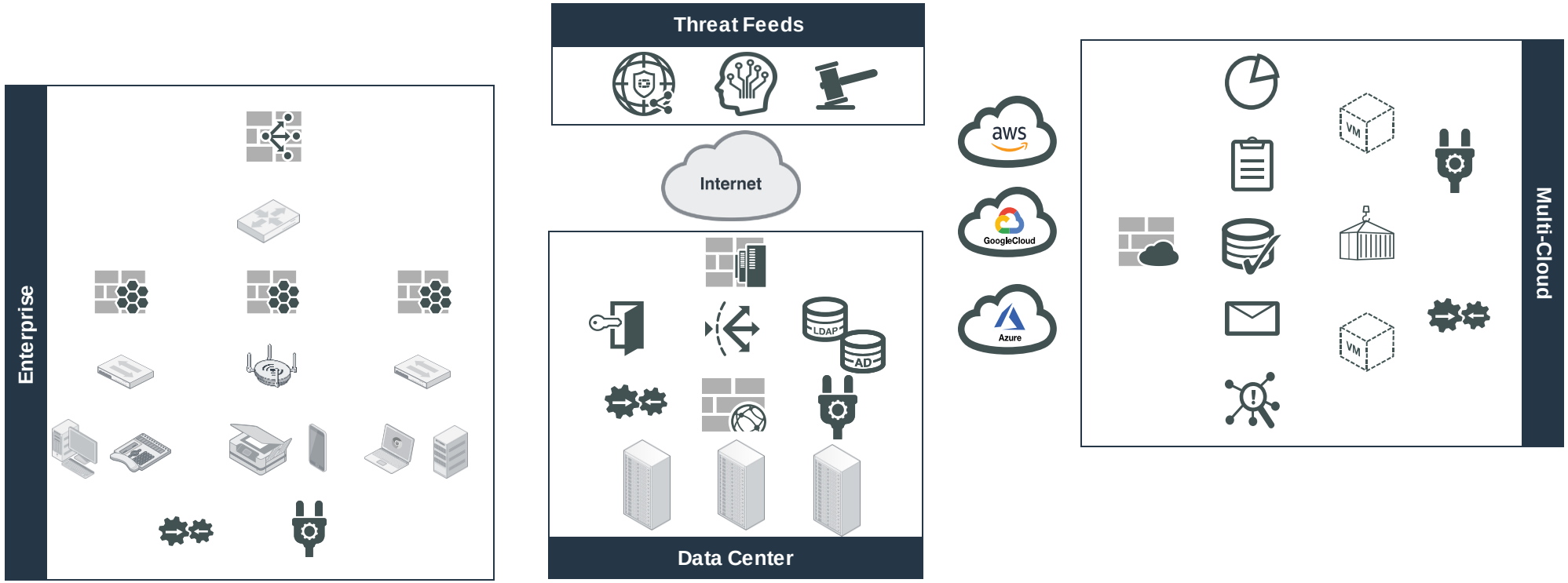
SSL Inspection Reputation App Control Content Filter

Network Security Critical Capabilities

- Threat Protection
- Content Visibility
- Identity & Access Management
- Security Intelligence
- Advanced Response (cusomization, automation)
- Networking Flexibility
- Network & Security Operations & Analytics
- Scalable Multi-Formfactor
- Open Ecosystem

© Fortinet Inc. All Rights Reserved.

Network Security Reference Architecture



Threat Protection

Antivirus | IPS | ATP | Anti-Spam | Anti-Botnet

Content Visibility

SSL Inspection | Reputation | App Control | Content Filter

Network Security Critical Capabilities

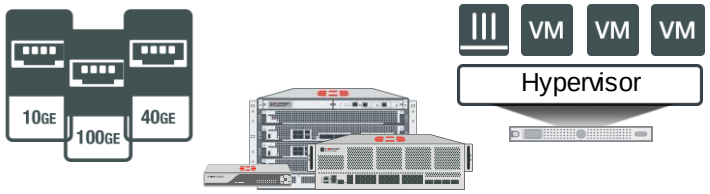
- Threat Protection
- Content Visibility
- Identity & Access Management
- Security Intelligence
- Advanced Response (cusomization, automation)
- Networking Flexibility
- Network & Security Operations & Analytics
- Scalable Multi-Formfactor
- Open Ecosystem

© Fortinet Inc. All Rights Reserved.

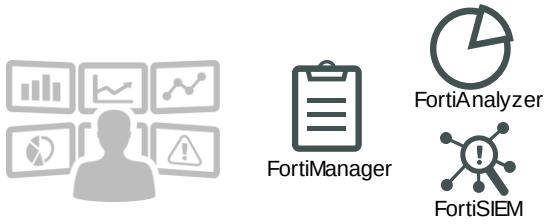
Fortinet Network Security Architecture Components

Open Ecosystem

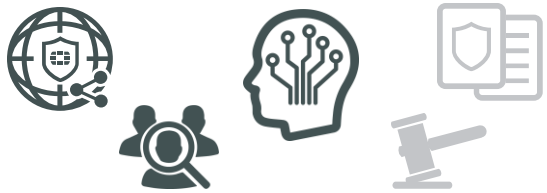
Scalable Multi-Formfactor



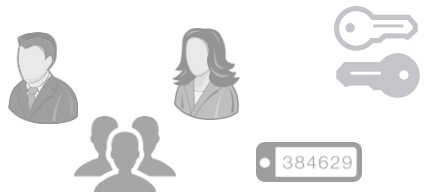
Network & Security Operations & Analytics



Security Intelligence

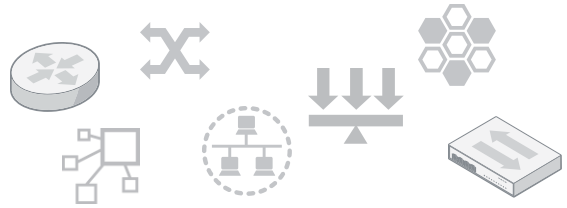


Identity & Access Management

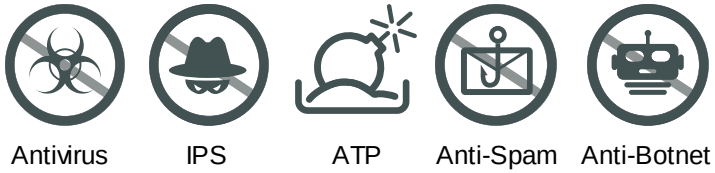


Advanced Response

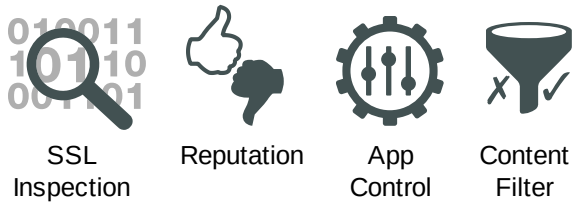
Networking Flexibility



Threat Protection



Content Visibility



Network Security Critical Capabilities

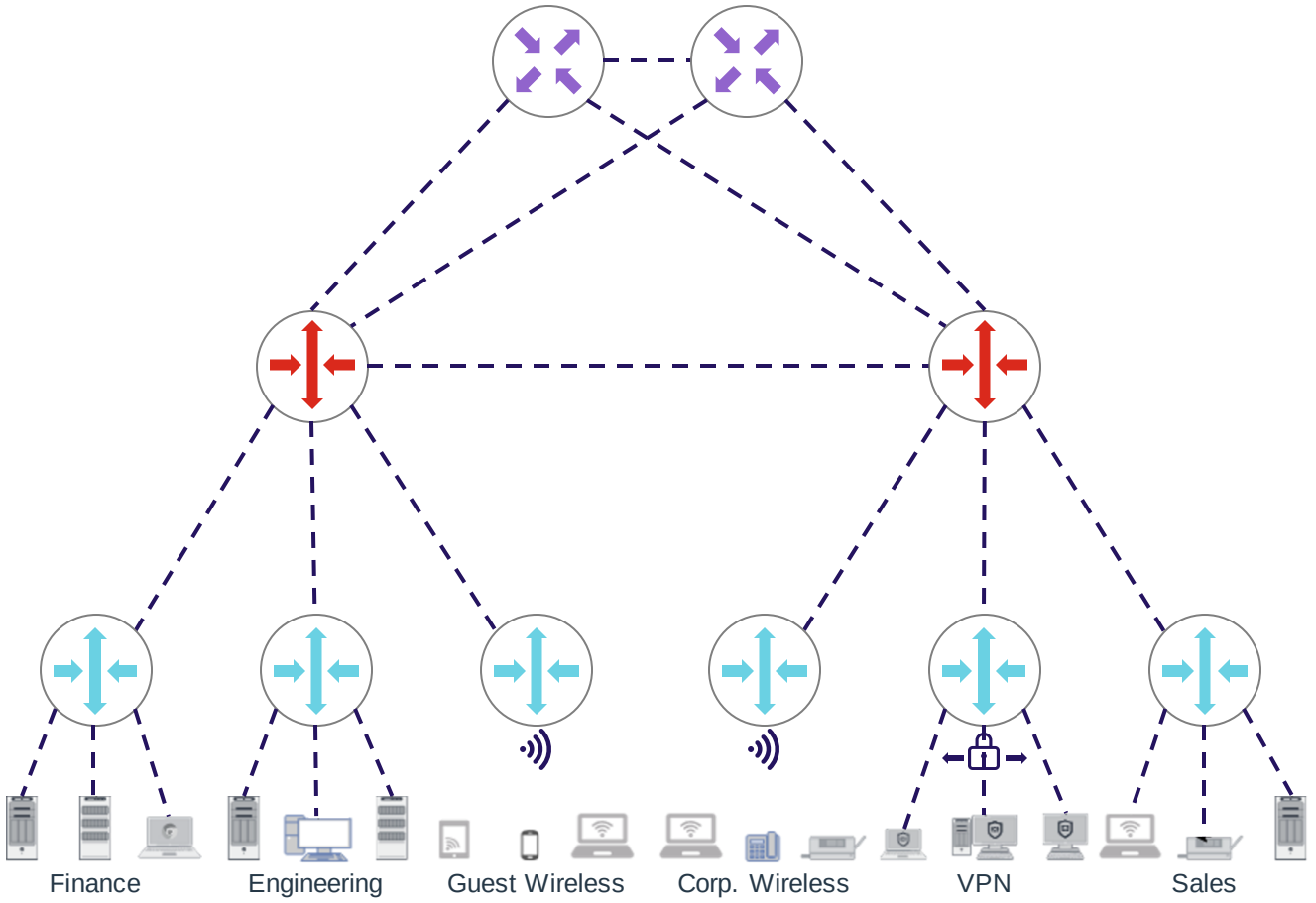
- Threat Protection
- Content Visibility
- Identity & Access Management
- Security Intelligence
- Advanced Response (cusomization, automation)
- Networking Flexibility
- Network & Security Operations & Analytics
- Scalable Multi-Formfactor
- Open Ecosystem

© Fortinet Inc. All Rights Reserved.

Segmentation Architectures

Use Cases Summary

Segmentation Architectures



© Fortinet Inc. All Rights Reserved.

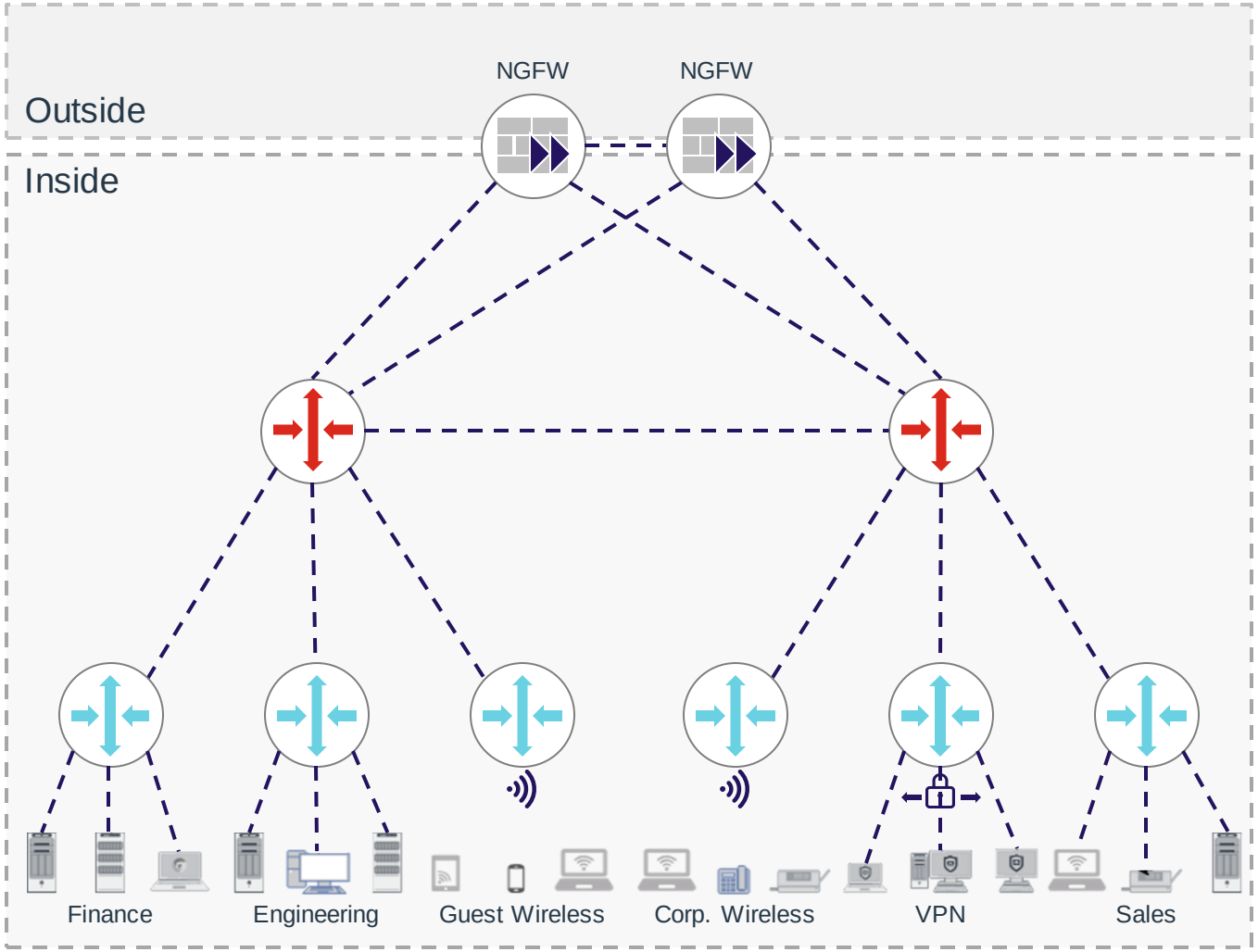
Today – Border Security

Problem

- Protect business from outside threats
- Protect users from the internet
- Keep users productive

Solution

- Apply all security at the internet edge
- ❖ Flat network provides no internal security
- ❖ Visibility into the network severely limited
- ❖ Risk of compromise is very high



Establishing Trust

- **Network Address**
- **User Identity**
- Business Logic
- Fabric Connectors
- **Applications**
- Device Identity

Advanced Security

- SSL Inspection
- **IPS**
- **Antivirus**
- **Application Control**
- **Web Content Filter**
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- Cloud Access Security Broker
- Advanced Threat Protection
- Endpoint Protection

© Fortinet Inc. All Rights Reserved.

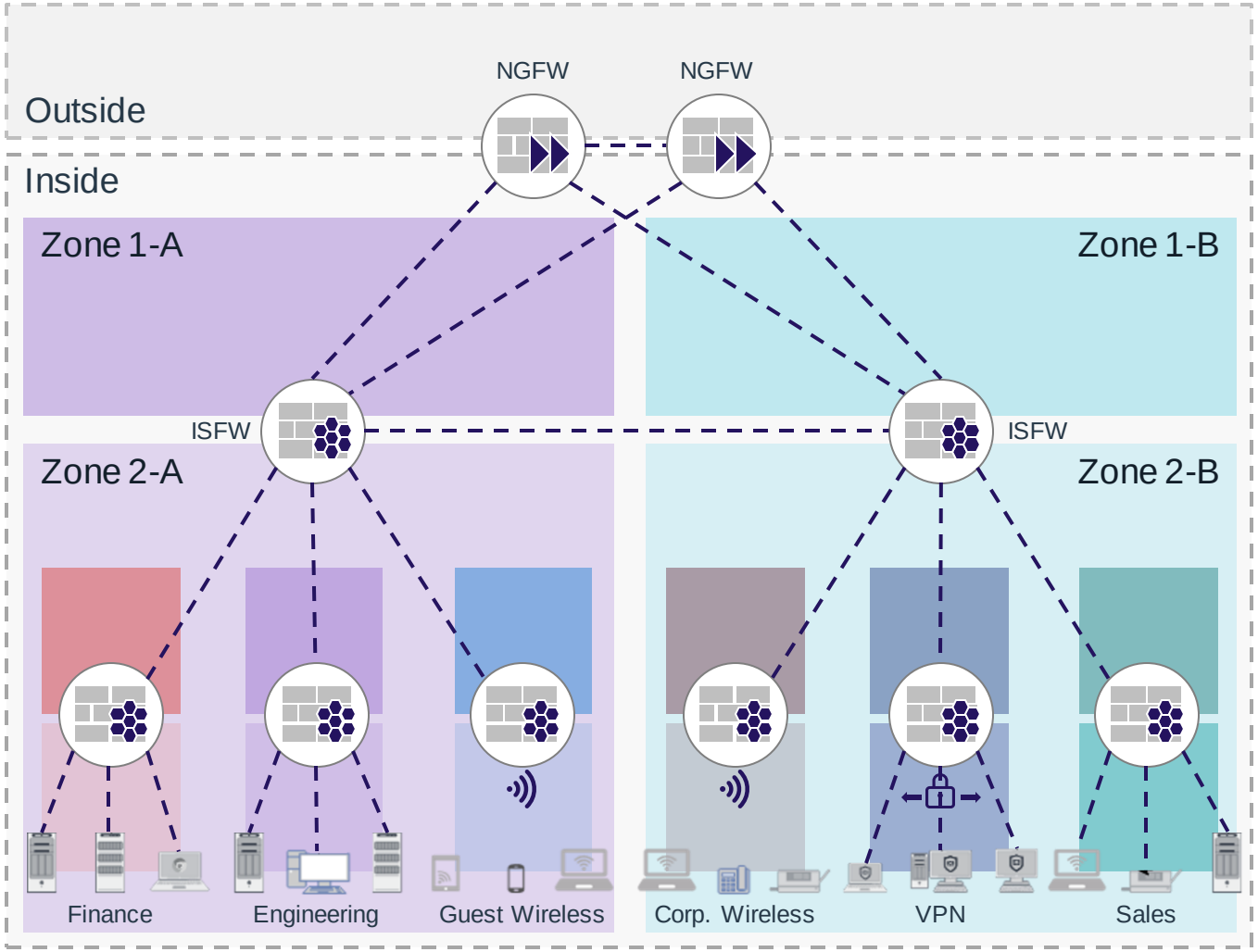
Use Case – Reducing Attack Surface

Problem

- Flat internal network
- No internal visibility
- No internal security

Solution

- Many Enforcement points
- Create containment zones
- Inspect SSL
- Inspect Applications
- Check for zero-day malware
- Protect critical assets



Establishing Trust

- Network Address
- User Identity
- Business Logic
- Fabric Connectors
- Applications
- Device Identity

Advanced Security

- SSL Inspection
- IPS
- Antivirus
- Application Control
- Web Content Filter
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- Cloud Access Security Broker
- Advanced Threat Protection
- Endpoint Protection

© Fortinet Inc. All Rights Reserved.

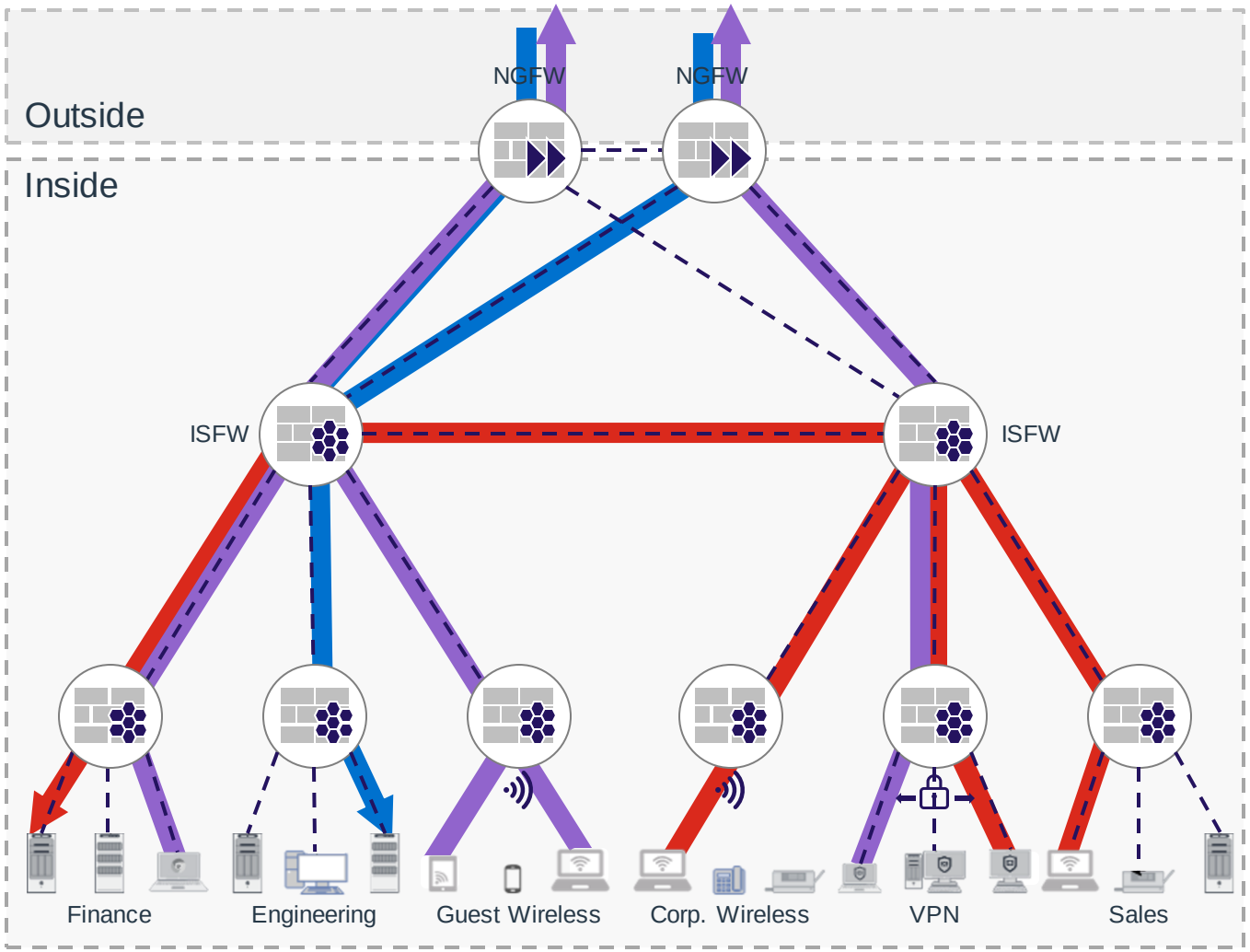
Use Case – Trusted Application Integrity

Problem

- Business critical applications must be secured
- Multiple applications
- Users in many locations

Solution

- Secure applications with solutions that share security intelligence
- Utilize security that will work with mobility and cloud usage
- Inspect SSL to make sure only trusted transactions are taking place
- Establish trust with sources inside and outside the network



Establishing Trust

- Network Address
- User Identity
- Business Logic
- Fabric Connectors
- Applications
- Device Identity

Advanced Security

- SSL Inspection
- IPS
- Antivirus
- Application Control
- Web Content Filter
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- Cloud Access Security Broker
- Advanced Threat Protection
- Endpoint Protection

© Fortinet Inc. All Rights Reserved.

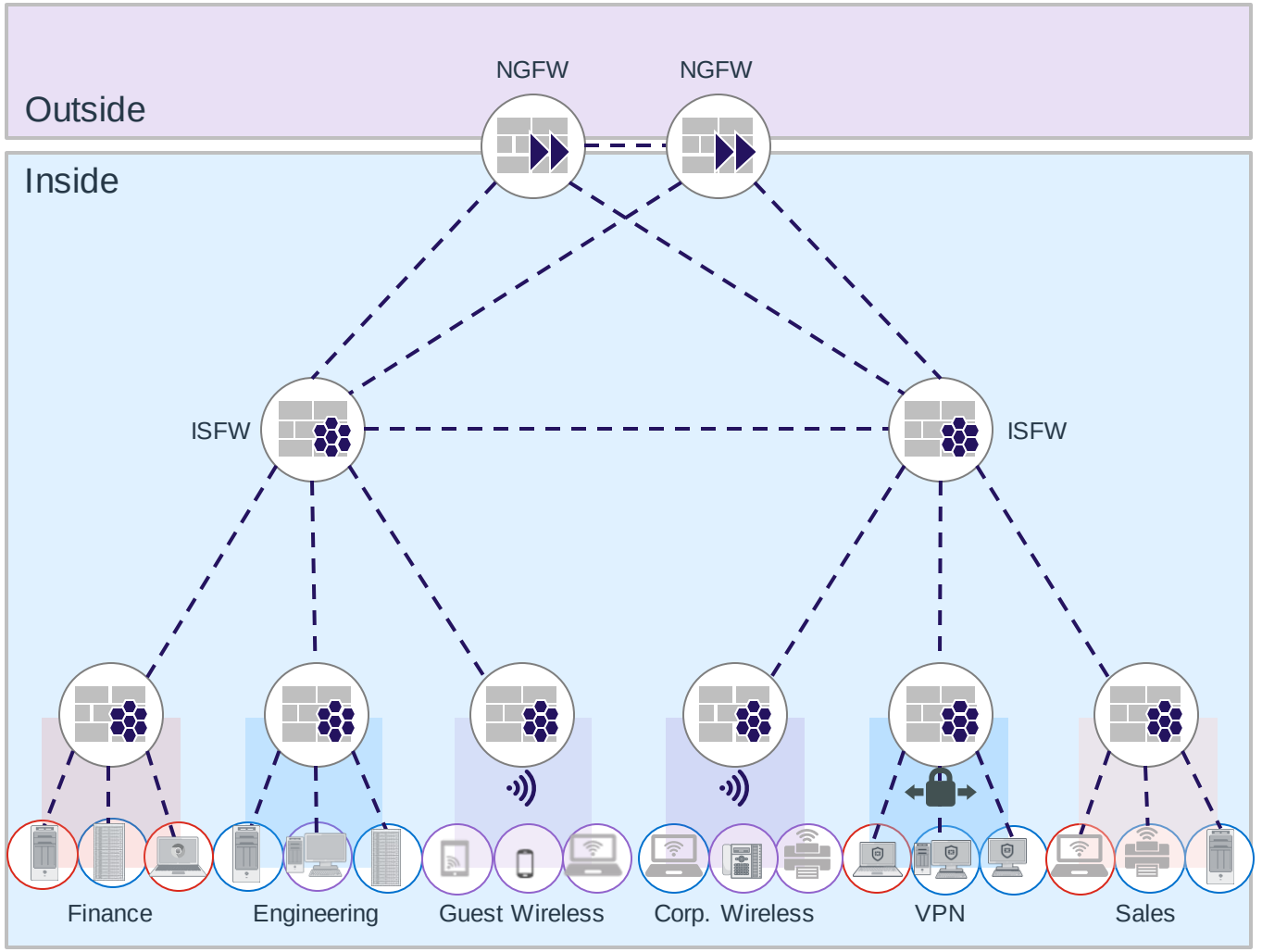
Use Case – Achieving Compliance

Problem

- Enforcing regulated access
- Does not follow standard network boundaries
- Critical compliance policies

Solution

- Multiple enforcement point locations
- Endpoint coverage for specific needs
- Network coverage for IoT
- Visibility for audits
- Keep critical systems running



Establishing Trust

- Network Address
- **User Identity**
- **Business Logic**
- Fabric Connectors
- Applications
- **Device Identity**

Advanced Security

- **SSL Inspection**
- IPS
- Antivirus
- Application Control
- Web Content Filter
- **Data Loss Prevention**
- Secure Email Gateway
- **Denial of Service Protection**
- Web Application Firewall
- Cloud Access Security Broker
- **Advanced Threat Protection**
- **Endpoint Protection**

© Fortinet Inc. All Rights Reserved.

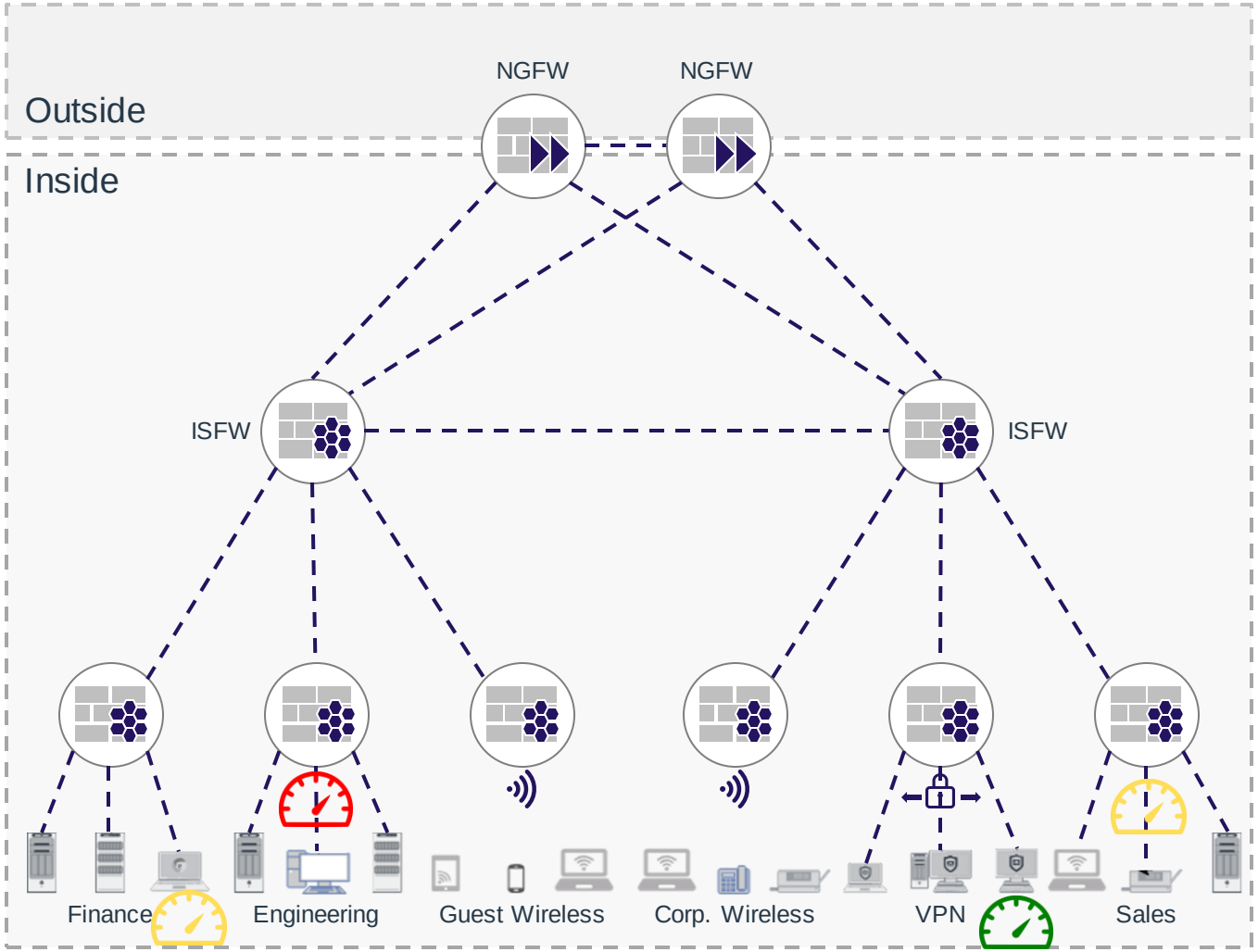
Use Case – Tiered Cloud Access

Problem

- Unexpected cloud costs
- Shadow IT
- No visibility of cloud data

Solution

- Combine cloud usage statistics with local enforcement
- Regulate access to cloud resources from authorized users
- Maintain audit trails of cloud hosted data
- Prevent data exfiltration



Establishing Trust

- Network Address
- **User Identity**
- Business Logic
- **Fabric Connectors**
- Applications
- Device Identity

Advanced Security

- SSL Inspection
- IPS
- Antivirus
- **Application Control**
- Web Content Filter
- **Data Loss Prevention**
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- **Cloud Access Security Broker**
- Advanced Threat Protection
- Endpoint Protection

© Fortinet Inc. All Rights Reserved.

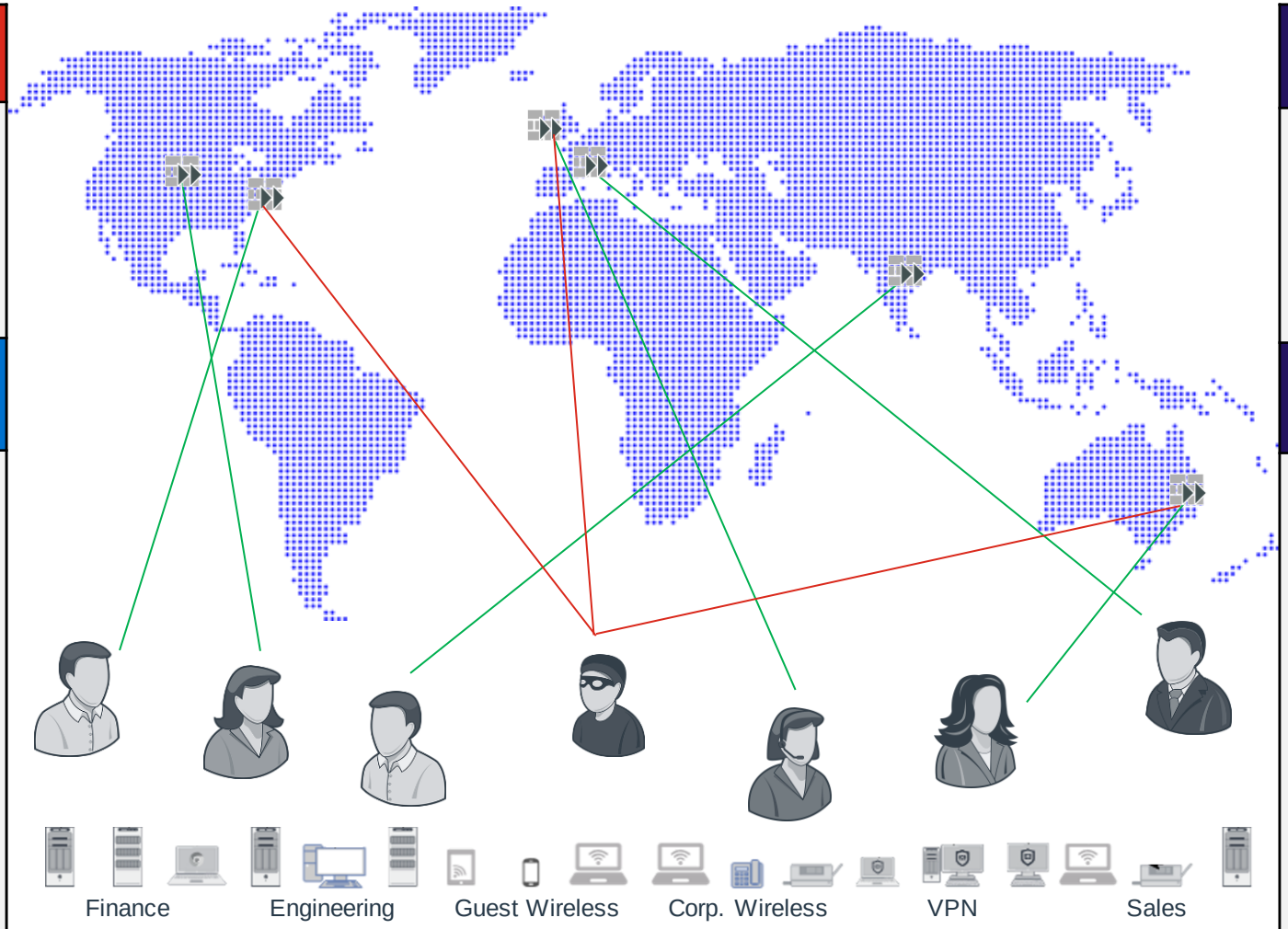
Use Case – Secure Physical Access

Problem

- Securing global employee presence
- Different systems control different aspects of security

Solution

- Integrate different trust sources
- Correlate physical location token information with network login location
- Maintain identity and device interrelationships
- Prevent targeted attacks



Establishing Trust

- Network Address
- **User Identity**
- Business Logic
- **Fabric Connectors**
- Applications
- **Device Identity**

Advanced Security

- SSL Inspection
- **IPS**
- **Antivirus**
- **Application Control**
- Web Content Filter
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- **Web Application Firewall**
- Cloud Access Security Broker
- **Advanced Threat Protection**
- Endpoint Protection

© Fortinet Inc. All Rights Reserved.

FORTINET