

Utilizing Zeek in an Enterprise Environment or for Distributed Operations

Designing a Zeek Deployment for Enterprise Monitoring



Michael Edie

Security Engineer

@tankmek blog.edie.io



Overview



Globomantics problem statement

- Zeek management



Configuring a Zeek Management Host



Zeek Management Host

Zeek installed

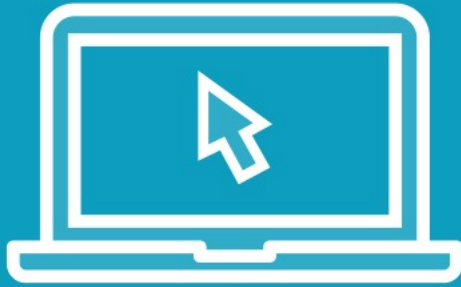
Create Zeek user

Generate SSH keys

Edit cluster configuration



Demo



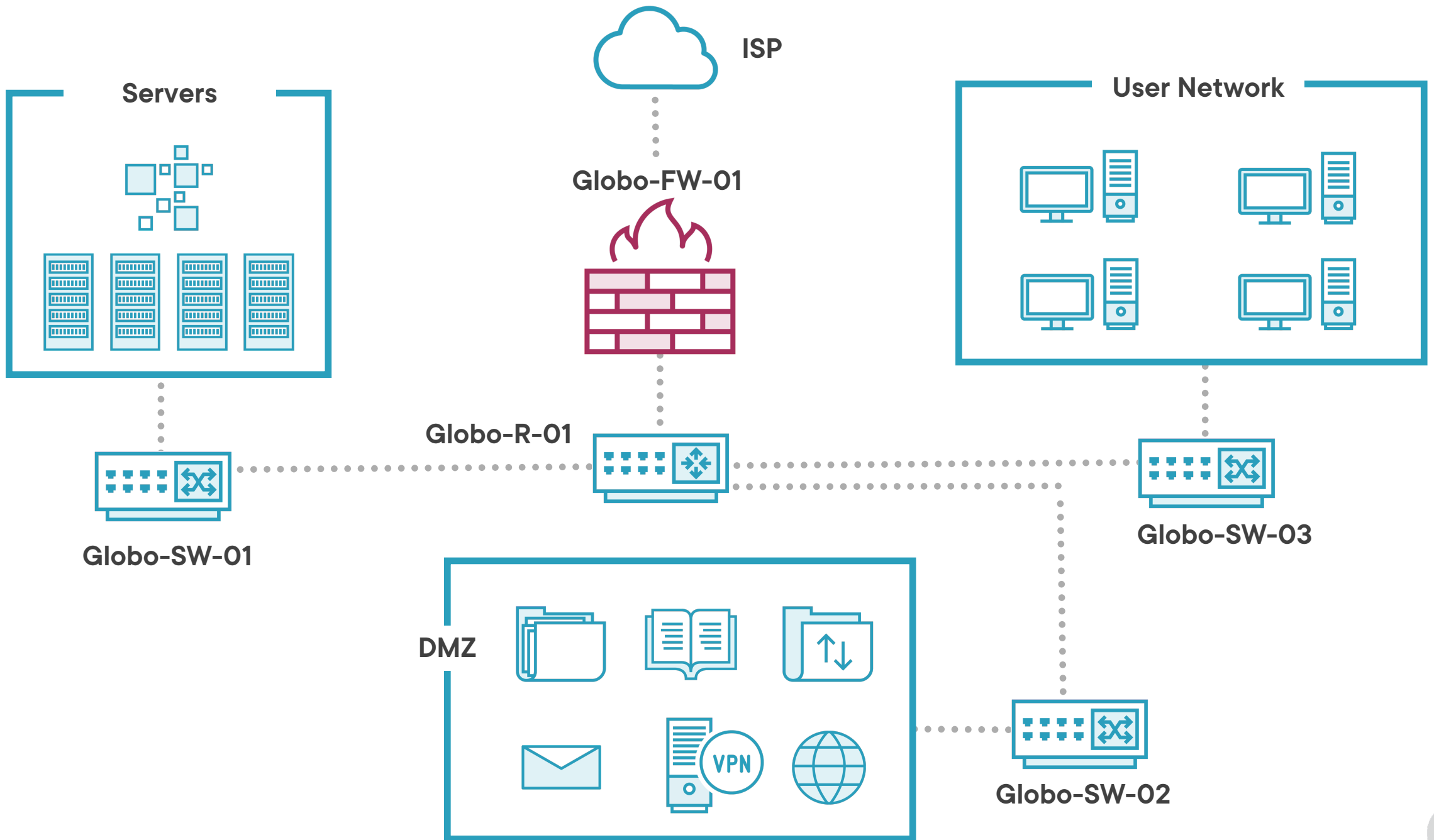
Zeek management host

- Verify Zeek install
- Create Zeek user
- Generate SSH keys
- Edit Zeek cluster configuration



Developing a Sensor Strategy





Connecting Zeek Workers to the Management Host



Zeek Sensors

Zeek installed

**Verify that everything
is installed, and
versions are the same**

Zeek user

**This is the user the
management host will
use to connect and
configure each sensor**

Packet capture permissions

**The Zeek software
needs certain
privileged permissions**



SERVER Sensor



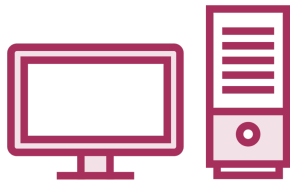
DMZ Sensor



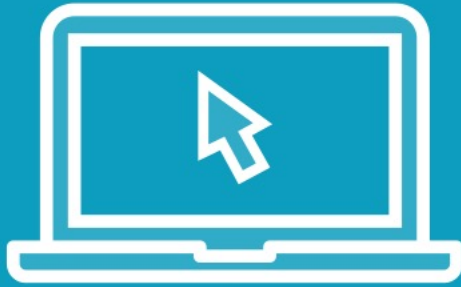
USER Sensor



**Zeek
Management**



Demo



Connecting sensors to management host

- Verify Zeek install
- Create Zeek user
- Configure raw packet capture permissions
- Deploy cluster configuration
- Validate logs on Zeek master



Working with the Filebeat Agent



Filebeat Agent

Install Filebeat

Setup Zeek plugin

Configure Zeek plugin

Output to Elasticsearch



SERVER Sensor



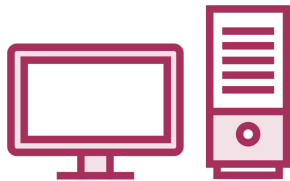
DMZ Sensor



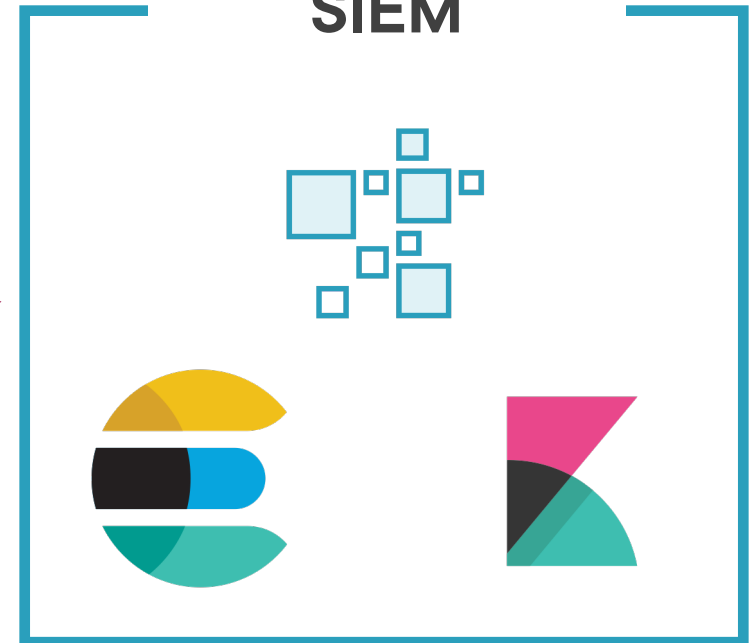
USER Sensor



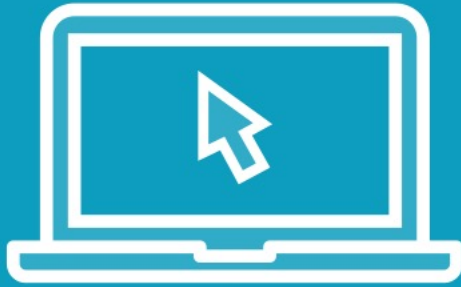
**Zeek
Management**



SIEM



Demo



Shipping Zeek data to a SIEM (ELK)

- Install Filebeat
- Install Zeek Filebeat plugin
- Configure Zeek plugin
- Configure Filebeat output to Elasticsearch



Summary



Zeek cluster architecture

- Management host
- Sensor strategy
- Deploy cluster configuration
- Ship Zeek data to SIEM