

Security Tools Report

CISY 7033 – 01

Dylan McCaffrey | Lucas Arias | Foster Alcantara

# Company Overview

Dylan McCaffrey | Lucas Arias | Foster Alcantara

Security Corporation provides security audits and services to organizations seeking to learn more about protecting their assets. We are located in Silicon Valley, California. We provide audits, intrusion research, network optimizations, and PAN configurations. Our certified team is dedicated to protecting your network in a cost effective and user friendly way. We currently employ 624 people with various departments within our organization.

|  |  |
| --- | --- |
| Department | Number of Employees |
| Accounting | 150 |
| Human Resource | 50 |
| Reception | 200 |
| IT | 50 |
| Customer Service | 174 |
| TOTAL | **624** |

We only operate in one centralized location therefore; we limit our corporate traffic to one centralized place. Our company requires several technology services and equipment to maintain a secure, fault tolerant facility.

# Services, Protocols, and Ports

In order to operate this large of a customer base, we take security very seriously. This means only the most explicit permissions will be allowed for the bare minimal ability for employees to complete their jobs.

|  |  |  |
| --- | --- | --- |
| Service | Port | Protocol |
| DNS | 53 | TCP,UDP |
| SSH | 22 | TCP |
| ICMP (diagnostics) | 7 | TCP |
| DHCP | 67, 68 | UDP |
| NTP | 123 | UDP |
| HTTP | 80 | TCP |
| HTTPS | 443 | TCP |
| PPTP | 1723 | TCP |
| GRE | 47 | TCP |
| SMTP | 465, 109, 110, 143 | TCP |
| Printer | 427, 137, 161 | UDP |
| 9100 | TCP |

We have an implicit deny on our PAN Firewall, providing enhanced security for our network. This works by blocking all traffic that isn’t directly allowed in our policy. We allow basic services such as DNS, DHCP, and ICMP for diagnostics to ping across our network. Additional services include:

* Network Time Protocol – to allow clock synchronization
* Hypertext Transfer Protocol – for standard web browsing
* Hypertext Transfer Protocol Secure – for secure web browsing
* Point to Point Tunneling Protocol – to allow VPN to the network
* Generic Routing Encapsulation – to aid VPN traffic
* Simple Mail Transfer Protocol – allows Gmail server

Users are only allowed to access terminals in their respective departments. Any other use is prohibited.

# Risk Identification

1. Internal Systems Compromised (Database, ADDS, Mail)
   1. Compromised systems cost the company money for analysis, customer identity protection, loss of trust in company, and prevents online sales and services
2. Web Applications
   1. Downtime of web services causes loss of sales, increased costs from remediation, decreased employee productivity
3. Core Services (DHCP, DNS)
   1. Downtime of core services cost employee productivity, increased cost of remediation, temporary loss of service

# Common Attacks

1. SQL Injection – This type of attack can compromise internal systems by damaging databases and compromising integrity
2. DDoS – This type of attack can interrupt web services temporarily until the attack is mitigated
3. DNS Poisoning- This attack can compromise DNS core services resulting in compromised systems and divert traffic to illegitimate destination
4. M.I.T.M. – This attack occurs when someone intercepts traffic and acts as the intended recipient controlling communication transparently
5. Brute Force – This attack occurs when someone attempts to guess password combinations, usually mitigated by implementing strict password policies and lockout rules.

# Security Compliance

In order to enforce our network policies, several security measures have been put into effect. We have included several security measures to protect our network including: Security Onion IDS, VLANs, IP Tables, and a Palo Alto Networks Firewall.

# Ring 1 (Internet Edge)

The PAN is the first point of contact for our network. This filters based on the security rules listed earlier. Any traffic that doesn’t match allow criteria is dropped. This Firewall is implemented on Layer 3. Virtual Router and DHCP is also the responsibility of the firewall. Connecting to the network are Gigabit ports allowing maximum throughput.

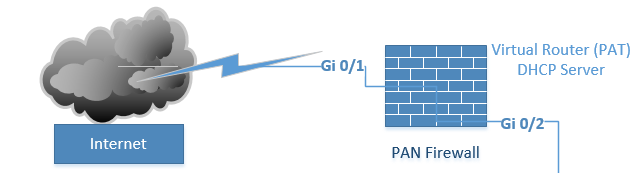
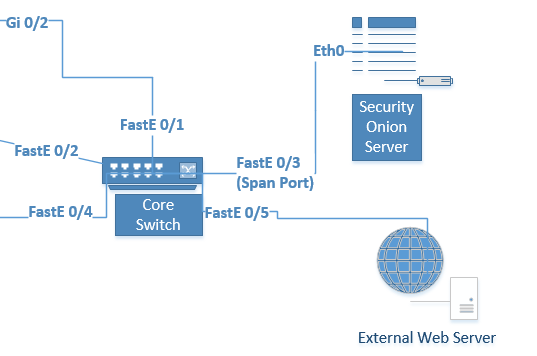


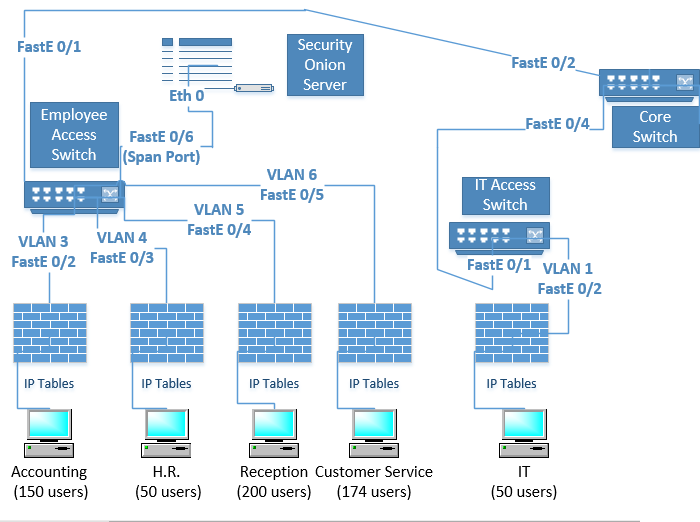
Figure 1

# Ring 2 (Backbone Edge)

Attached to our Core switching fabric is an NIDS (Security Onion) attached to a SPAN port. This port replicates all traffic through the switch allowing all traffic to be monitored. Also attached is our proxy web server which if brought down can be re-imaged.

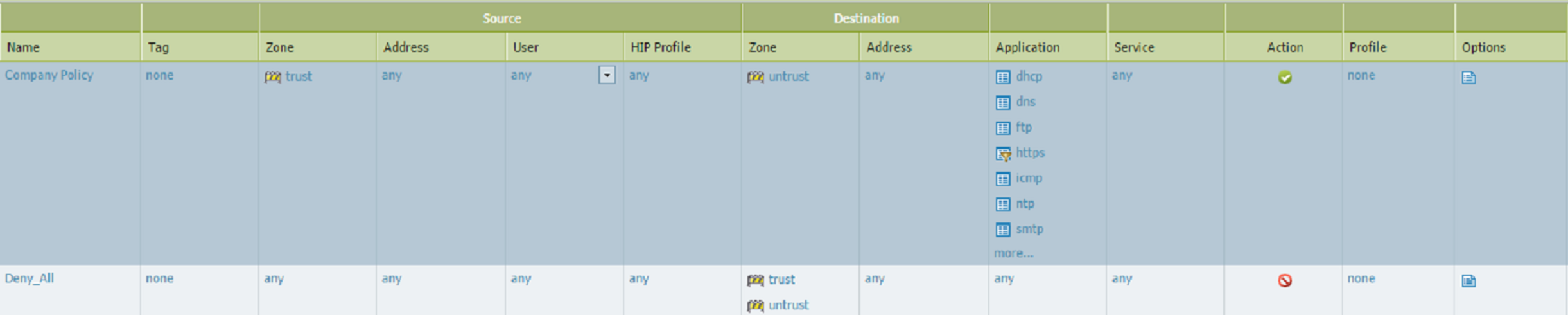
Figure

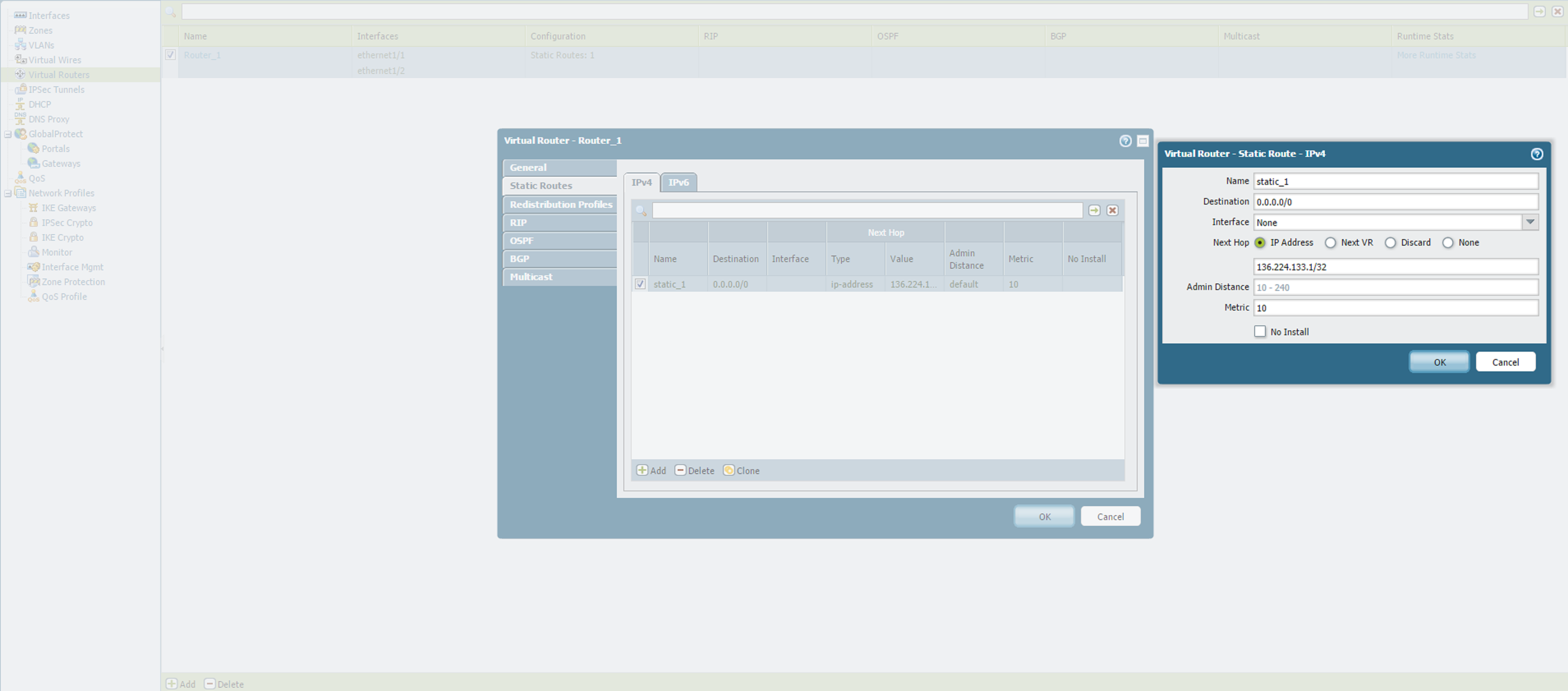
# Ring 3 + 4 (Network Edge + Host Security)

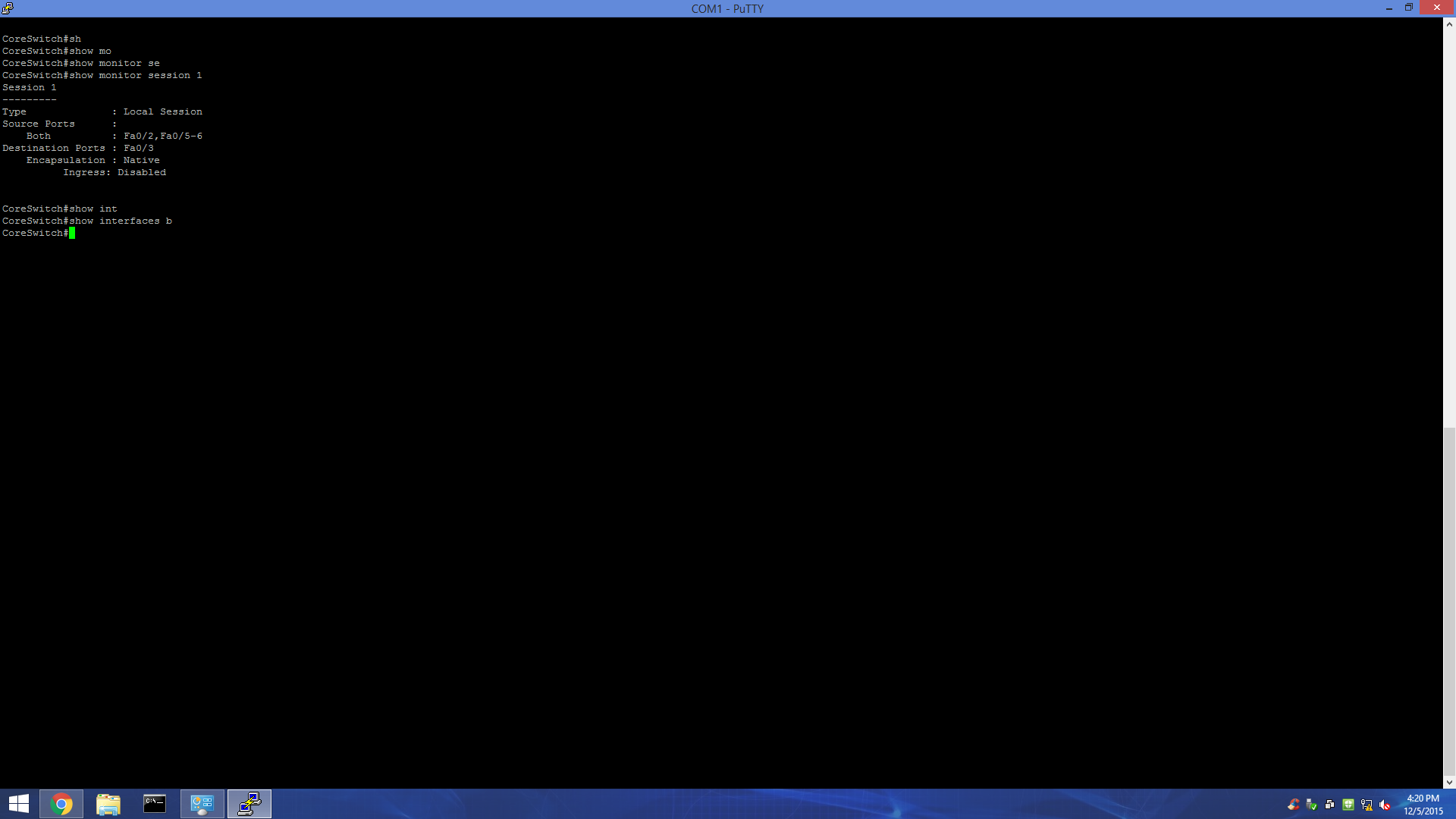
Our Access switches, workstations, and servers reside here. We have included host firewalls via iptables. Also VLANs are enabled on the switches, allowing filtering of traffic between trunks. Attached to the Employee Switch is an additional IDS to monitor traffic.

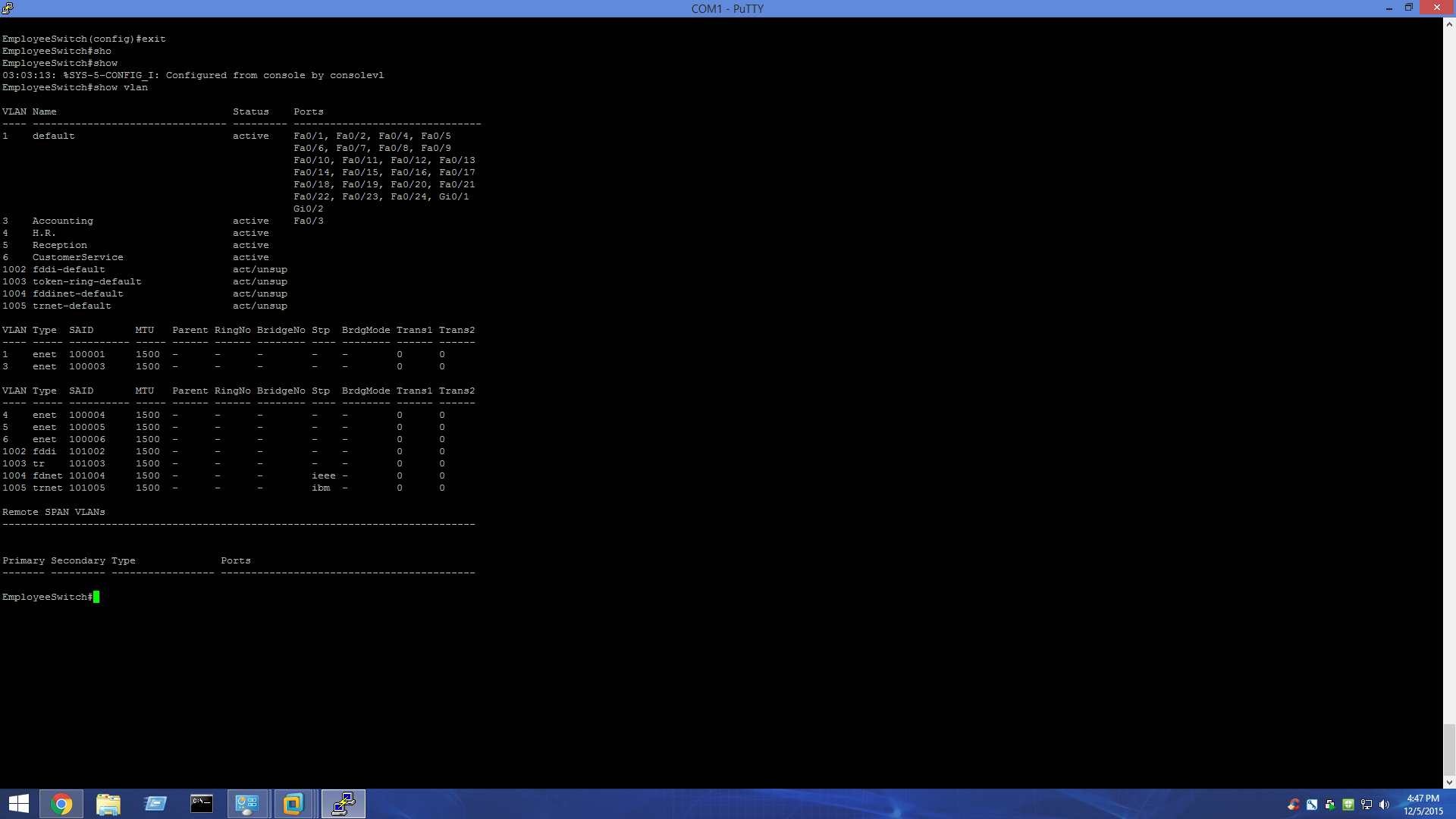
Figure

# Configurations

Palo-Alto Networks Firewall Security Policy

Palo-Alto Networks Firewall Virtual Router

Switch



Security Onion