

Asko Hakkarainen

# Cybergame firewall design and implementation

Bachelor's Thesis  
Information Technology

2017

<b>Tekijä/tekijät</b>	<b>Tutkinto</b>	<b>Aika</b>
Asko Hakkarainen	Insinööri (AMK)	Toukokuu 2017
<b>Opinnäytetyön nimi</b>		41 sivua 8 liitesivua
Cybergame firewall design and implementation		
<b>Toimeksiantaja</b>		
Kaakkois-Suomen ammattikorkeakoulu		
<b>Ohjaaja</b>		
Lehtori Vesa Kankare		
<b>Tiivistelmä</b>		
<p>Tämän opinnäytetyön tavoitteena oli suunnitella ja rakentaa toimiva, redundanttinen (kahdennettu) "North-South-palomuurijärjestelmä" Cybergame-projektiin, joka on Kymenlaakson ammattikorkeakoulun hanke. Palomuurijärjestelmän on tarkoitus reitittää ja rajoittaa Cybergamen sisäistä liikennettä eri virtuaalisten lähiverkkojen välillä.</p> <p>Työ keskittyi lähes kokonaan palomuurijärjestelmään, joka sisältää kaksi kappaletta Ciscon ASA 5515-X -sarjan laitteita. Muutamaa virtuaalista TinyCore Linux -konetta käytettiin virtuaalisten lähiverkkojen (VLAN) välisen liikenteen testaamiseen.</p> <p>Työssä käytettiin ASA 5515-X -laitteiden tukemaa Multiple context modea, jonka avulla kyseisen fyysisen palomuurin voi jakaa useaksi virtuaaliseksi palomuuriksi, kontekstiksi. Konteksteja työssä on kaksi kappaletta, jotka erittelevät virtuaaliset lähiverkot toisistaan. Kahdentamista varten työssä käytettiin kahta failover-tekniikkaa: stateless ja stateful. Sisäistä liikennettä rajoitetaan pääsylistoilla, jotka tällä hetkellä sallivat kaiken IP-liikenteen.</p> <p>Työ oli onnistunut siihen pisteeseen, mihin tällä hetkellä pystyi. Cybergame ei ole valmis, joten pelin sisäistä liikennettä ei voida seurata eikä voida tutkia, millaista liikennettä pitää sallia pääsylistoilla. Työssä käydään kuitenkin läpi, kuinka liikenteen monitoroinnin tulisi tapahtua. Palomuurijärjestelmän kahdennus testattiin lähettämällä jatkuva ICMP-ping työasemalta, minkä aikana aktiivinen palomuuuri käynnistettiin uudelleen. Tällä tavalla huomattiin, että kahdennus toimii, sillä toinen laite vastasi ping-kyselyyn muutaman sekunnin jälkeen. Kahdennuksen toimivuuden voi testata myöhemmin suuremmalla liikennemäärällä, kunhan Cybergame on valmis.</p>		
<b>Asiasanat</b>		
Cybergame, virtualisointi, palomuuuri, VLAN, kahdennus		

<b>Author (authors)</b>	<b>Degree</b>	<b>Time</b>
Asko Hakkarainen	Bachelor of Engineering	May 2017
<b>Thesis Title</b>		
Cybergame firewall design and implementation		41 pages 8 pages of appendices
<b>Commissioned by</b>		
South-Eastern Finland University of Applied Sciences		
<b>Supervisor</b>		
Vesa Kankare, Senior lecturer		
<b>Abstract</b>		
<p>The purpose of this Bachelor's thesis was to design and implement redundant, North-South -firewall system into Cybergame project. The need for the firewall system is to route and permit/deny traffic inside Cybergame network between different virtualized local area networks, VLANs.</p> <p>The focus was solely on the firewall system, which consists of two Cisco's ASA 5515-X -models. A few virtualized TinyCore Linux's were needed for testing the connectivity between VLANs.</p> <p>The main protocol in the work was ASA 5515-X's Multiple context mode, which allows the firewall to be divided into multiple virtualized firewalls, contexts. Two contexts which separate VLANs from each other were used. These contexts are also referred as additional security layers. Inside traffic is restricted with access lists which at the moment, permit all IP traffic. For redundancy, two different type of failovers were used: stateless and stateful.</p> <p>The work was successful as far as it could as Cybergame is not ready. Traffic inside the game cannot be monitored to see what type of traffic goes there. All other traffic will then be denied with access lists. The thesis explains how the traffic could be monitored. Redundancy of the firewall system was tested by sending continuous ICMP-ping from a workstation and during that time, active firewall was rebooted. The other firewall replied to ping after a couple of seconds which meant that the redundancy worked. Redundancy could be tested later with much larger traffic when Cybergame is ready.</p>		
<b>Keywords</b>		
Cybergame, virtualization, firewall, VLAN, redundancy		

## TABLE OF CONTENT

1	INTRODUCTION .....	7
2	GYBERGAME PROJECT .....	8
2.1	Project overview .....	8
2.2	Cybergame design.....	9
2.2.1	Frontend.....	10
2.2.2	NEST .....	10
2.2.3	Backend .....	11
2.2.4	Management .....	11
2.3	Virtualization in Cybergame .....	11
3	TERMINOLOGY .....	12
3.1	VLAN .....	12
3.2	PVLAN.....	13
3.3	LACP .....	14
3.4	Multiple context mode.....	15
3.5	Failover.....	15
3.6	SSH .....	17
3.7	RADIUS .....	17
3.8	ASDM .....	17
3.9	NTP .....	18
3.10	Tiny Core Linux (OS).....	19
4	FIREWALL IMPLEMENTATION.....	20
4.1	Cisco ASA 5515-X.....	20
4.2	Installation and initial configurations .....	20
4.3	Logical topology.....	22
4.4	Failover configuration .....	23
4.5	LACP configuration.....	24
4.6	Context configurations .....	25
4.7	ASDM .....	27

4.8	Protocol configurations .....	27
4.8.1	NTP .....	27
4.8.2	RADIUS.....	28
4.8.3	Syslog .....	30
4.9	PVLAN configuration .....	31
4.10	ACLs.....	32
4.10.1	Creating and testing access lists.....	32
4.10.2	Monitoring traffic .....	34
4.11	Failover test .....	35
5	CONCLUSION.....	38
	REFERENCES .....	40

## APPENDICES

Appendix 1. Admin-context configuration

Appendix 2. System-context configuration

Appendix 3. Level1-context configuration

Appendix 4. Level2-context configuration

## ABBREVIATIONS

ADC	Application Delivery Controller
ACE	Access Control Entry
ACL	Access Control List
ASDM	Adaptive Security Device Manager
DDoS	Distributed Denial of Service
GUI	Graphical User Interface
HA	High-Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LACP	Link Aggregation Control Protocol
NTP	Network Time Protocol
OS	Operating System
PVLAN	Private Virtual Local Area Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UI	User Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMM	Virtual Machine Monitor

## 1 INTRODUCTION

Gamification is making its way to be part with learning as it is instructive and it could be fun. Cybergame was an idea to combine two things: learning and playing a game. What could be more fun than playing a game in school and still you get awarded with credits? The idea of this bachelor's thesis came from a senior lecturer Vesa Kankare at the Kymenlaakso University of Applied Sciences (KyUAS). This thesis is part of Cybergame project that requires strong protection from the outside network and needs to have separated security layers to protect and pass the traffic within the game. Cybergame network is completely isolated within CyberLab's production network. CyberLab is a cybersecurity laboratory located in the Information Technology Department at KyUAS. In this thesis, two Cisco ASA 5515-X firewalls are used to make the security layers redundant.

There are a few work-in-progress thesis works on Cybergame as it is a big project. The game itself is not ready but the network infrastructure for it almost is. This thesis is focused on the security layers in Cybergame network which are separated with firewalls. Other notable work-in-progress thesis' are virtualization and Application Delivery Controllers in Cybergame network. Since those thesis' are part of the project, they are explained very shortly in this thesis. Published and the most recent thesis is Antti Peltonen's Application Delivery Controller Implementation to Cyberlab Data Center (Peltonen 2016).

The firewalls were installed in Cybergame server rack in CyberLab and were connected together via failover-link so the redundancy can be configured later. After that, they were connected to two Cybergame switches with load balancing etherchannel to pass the normal network traffic between clients and Cybergame. Finally, a management switch was installed and both firewalls were connected to it to separate normal network traffic from management traffic.

After this introduction, Cybergame project design and some of its history will be explained in Chapter 2. Chapter 3 is "Terminology" which consists of most used terms or protocols in the thesis and are also explained. Chapter 4 focuses on the implementing of firewalls to the Cybergame infrastructure and configuring them. Configurations are in appendices.

## 2 GYBERGAME PROJECT

### 2.1 Project overview

In early 2015 a project Cybersecurity Expertise and Business Development was started to combine datacenter, gamification and cybersecurity knowledge. Some of the project's goals are new research and learning possibilities of cybersecurity, Cybergame and CyberLab. The project is funded by European Regional Development Fund (ERDF) (Euroopan aluekehitysrähoitus 2014).

CyberPros Academy was started in May 2015 with the cooperation of KyUAS, Lappeenranta University of Technology (LUT) and Cursor Ltd. Its idea is to create an environment to study different kind of cybersecurity threats and how to prevent them. For this the CyberLab laboratory and cybersecurity class room were created in KyUAS. This project has an extremely important role in studying cybersecurity today. (Rouhiainen & Kettunen 2015.)

In the CyberLab environment it is also possible to do and study penetration testing and vulnerability scanning which are crucial part of cybersecurity today (Rouhiainen & Kettunen 2015). Antti Peltonen did a DDoS test as a part of his bachelor's thesis in CyberLab environment and the attack was made by students mainly with TCP SYN flood and Slowloris (Peltonen 2016).

Cybergame designing started in the late 2015 and the game will mainly be developed by students. Game designers will work on the game itself with help from GoodLife Technologies, a partner in the project. Networking students will work on the network infrastructure. (Rouhiainen & Kettunen 2015.)

Cybergame is a gamified environment for learning cybersecurity and use of penetration techniques to bypass different security layers. The game consists of scenarios where players need to score points by completing steps, which are set by game developers. Usually, the main goal is to gain access to the target network and get information out of it using penetration testing tools, like in Kali Linux. (Peltonen 2016.) Steps can be like "get the password for user x" or "gain access to security cameras".

The reason for the topic of the execution of this bachelor's thesis is that Cybergame must be protected from malicious users so hacking the game itself will be more difficult. For example, the player database must be protected



from unauthorized access so no one can alter the scores. Now the network of the game is only available for the students of IT department and can only be accessed from the IT department network. Even though it is an inside network, it is still seen as the untrusted network from the perspective of Cybergame network.

## 2.2 Cybergame design

Cybergame itself is protected from the Internet by Application Delivery Controllers. Their function is to redirect traffic to servers and NEST (See chapter 2.2.2 for more info), handle web security and DoS protection. ADCs will also perform SSL offloading for web-based services to reduce load from the servers and simplifies certificate management.

North-South firewall (from least secure to most secure) will protect the flowing traffic through different security layers inside Cybergame datacenter. These security layers are separated by virtual firewalls and in Cisco ASA they are called contexts. Contexts are named Level1 and Level2, which will be explained in the implementation chapter. See figure 1 for Cybergame topology.

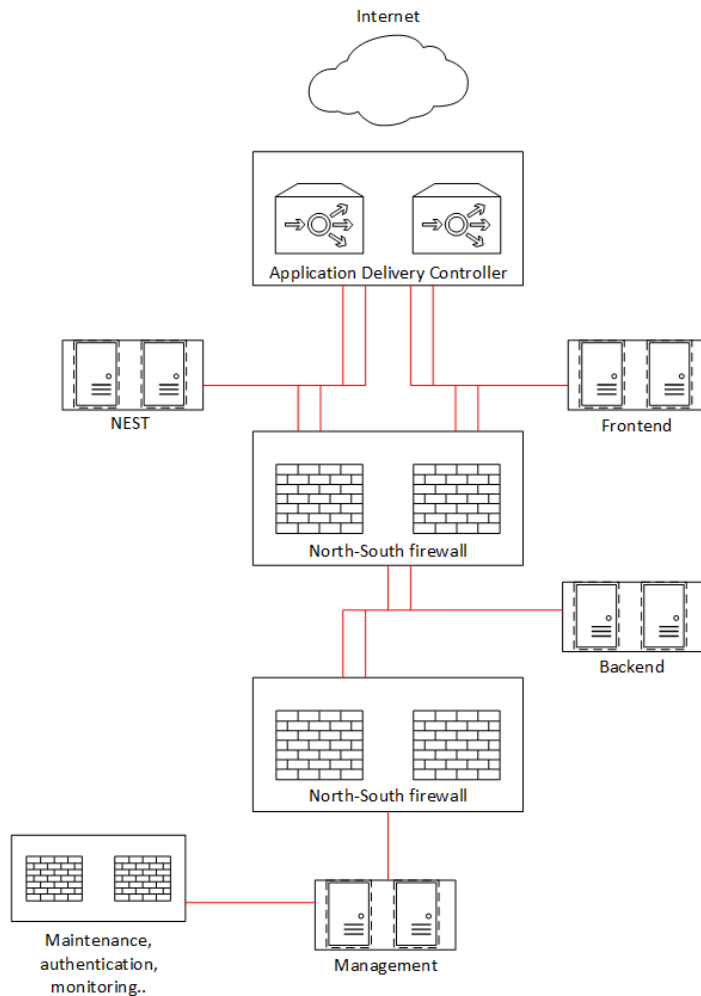


Figure 1. Cybergame topology

### 2.2.1 Frontend

Frontend is a server that hosts web interface for Cybergame. This is the interface between user and game server (in this case, Backend. Chapter 2.2.3). Connections from Frontend towards Backend are allowed, while no other connections are. Frontend is everything a user can see or interact with which makes it UI for the game. For example, when you access to Cybergame as a user, the first thing you face is Frontend. In Cybergame it is accessed via browser using a secured http -connection. After that, it will ask you to log in to authenticate yourself to access the game.

### 2.2.2 NEST

All the scenarios are run in the NEST network. NEST is a VM running hypervisor (chapter 2.3) which runs all Cybergame scenarios and scenario VMs.

NEST is not allowed to initiate any connections, only Backend connections towards NEST are. After authenticating, a scenario can be chosen from the UI. If the scenario is completed or paused, it will store all the information to the database so the scenario can be replayed or resumed later.

### 2.2.3 Backend

The Backend is the database of the game where all the users' information is. User cannot see or interact with Backend but all the information is retrieved from there. Some of the information may be seen in UI (it is up to game developers how they want to make it) like completed scenarios and scores a player's got or someone else's high score on that specific scenario. A user must not have access to other users' information.

### 2.2.4 Management

Management is only used for management access and maintenance. Users that have privileges (mainly staff) can access the management interface. It can be used for example, monitoring or upgrading the system and security components which is why it is needed to be the most secure. Management is behind Backend, and is invisible to players. Management must be protected from unauthorized access and Internet access is denied.

## 2.3 Virtualization in Cybergame

In short, virtualization technology means that multiple VMs can be run on one computer. The resources of the host computer are shared with multiple operating systems. Resource sharing is handled by a hypervisor. (VMware N.d.)

Hypervisors (or VMMs) are divided into two types. Type-1 hypervisor is a bare metal hypervisor that runs on top of hardware for example as an OS. Type-2 hypervisor operates as an application on already existing OS. (Techtarget 2010.) With virtualization technology, the need for hardware can be reduced which makes this cost-efficient solution.

In Cybergame, VMware ESXi is used and it is a type-1 hypervisor which makes it like an operating system. Four physical DELL-servers are used as hypervisors as all of them have ESXi installed. DELL-servers are also storage for Cybergame VMs which are installed on ESXi's. VMware vCenter was needed to manage and monitor the ESXi-servers. It is virtualized and is installed on one of the ESXi's. All the ESXi-servers were then added to vCenter library and were then added in to a cluster. Inside the cluster, ESXi-servers are using High Availability (HA) and load balancing.

HA means that even if one of the ESXi's inside the cluster shuts down for whatever reason, all the VMs on that ESXi-server move to another ESXi-server automatically. HA makes servers redundant. VMs can also be moved within the cluster while they are running. Load balancing means that vCenter's algorithm measures the load on all of the cluster's servers and balances them automatically. For instance, there are 100 VMs running on one of the ESXi's and zero VMs on all other three so vCenter balances them.

Cybergame and all the scenarios will be virtualized and will be added to the Cybergame cluster.

### 3 TERMINOLOGY

The most used or important protocols and terms in this thesis are explained in this chapter.

#### 3.1 VLAN

Local area network (LAN) consists of all the devices that are in the same broadcast-domain. This means that every device connected to the same broadcast-domain can receive broadcast-frames sent from other devices. A switch thinks that all of its access ports are in the same broadcast-domain, which means that all the devices connected to the switch are in the same local area network. To make the switch have more than one broadcast-domain, Virtual LANs are needed to be made inside the switch. (Odom 2008, 10.)

Broadcast-frames are sent to every network device in the broadcast-domain so in a large broadcast-domain that would make a lot of traffic. For example in a company it would be a wise decision to split the broadcast-domain into smaller ones: for example management, staff and production, a subnet for each department. With VLANs devices from different departments can be connected to the same switch without making traffic that could interfere with other broadcast-domains.

In Cybergame, there are four VLANs: NEST, Frontend, Backend and Management. Each of them has been assigned a different subnet with a prefix 21xx:

NEST: 172.16.0.0 /16 with a VLAN ID 2160

Frontend: 172.18.0.0 /24 with a VLAN ID 2180

Backend: 172.18.1.0 /24 with a VLAN ID 2181

Management 172.18.2.0 /24 with a VLAN ID 2182

### 3.2 PVLAN

Private VLAN divides a regular VLAN domain into subdomains. The regular VLAN domain is a primary VLAN and subdomains are secondary VLANs. These secondary VLANs are called an isolated VLAN and a community VLAN is seen in figure 2. All the PVLAN pairs share the same primary VLAN but can be separated from each other with secondary VLANs. Isolated VLAN means that ports associated with it cannot communicate with each other at the Layer 2 level. In opposed to isolated VLAN ports, all ports in community VLAN can communicate with each other. However, community ports cannot communicate with ports associated with other communities at the Layer2 level. (Cisco N.d.a.)

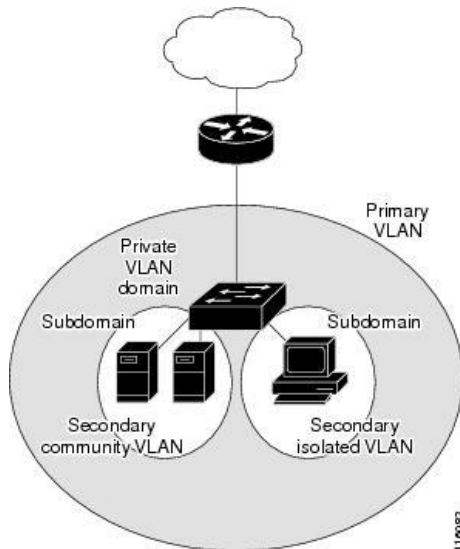


Figure 2. Private VLAN domain (Cisco N.d.a.)

In Cybergame project, there are only isolated secondary VLANs with a prefix 22xx:

NEST 2260

Frontend 2280

Backend 2281

Management 2282

### 3.3 LACP

LACP is link aggregation protocol to bundle physical links into a logical one (IEEE Standards Association 2001). With this protocol, the bandwidth between two devices can be increased and it has automatic load-balancing across the other operational links if a failure is detected in one link. Cisco has copyrighted term EtherChannel that is a link aggregation technology. EtherChannel is used in Cisco devices, which can be configured with LACP or with a Cisco proprietary protocol: Port Aggregation Protocol (PAgP). (Omnisecu N.d.) LACP is used in this work.

### 3.4 Multiple context mode

A single ASA can be partitioned into multiple virtual firewalls, called security contexts. Each context is like an independent firewall with its own security policies, interfaces and management. This is equivalent to have multiple standalone devices. (Cisco N.d.d.) Multiple contexts have several pros and cons, which are listed below.

Pros of multiple contexts:

- Can be used if various departments or users need their own context or security policies
- Hardware requirements
- Active/Active failover (See chapter 3.5)

Cons of multiple contexts:

- No dynamic routing protocols, only static routes
- No Threat Detection
- No multicast routing
- No VPN for remote access, only site-to-site VPN tunnel
- No QoS (Cisco N.d.d.)

After enabling multiple context mode and rebooting the device, it boots with system context, admin context and with additional security contexts depending on a license. The default license allows two additional security contexts. System context is used to configure each context configuration location, allocated interfaces and context operating parameters (startup configuration in single mode). If a user access to admin context, it gains privileges to access system context and all other contexts. Therefore, access to the admin context should be limited to appropriate users. (Cisco N.d.d.)

### 3.5 Failover

Failover is a HA technique. In failover, two devices are connected to each other with a cable, a dedicated failover link. Failover monitors the health of active units and interfaces if specific conditions are met. If not, failover occurs. In order for failover to work, both devices need to be exactly the same: model, interfaces, modules (if any) and have the same amount of RAM installed. Also on software: firewall mode (routed or transparent), context mode (single or multiple) and have the same software version. (Cisco N.d.e.)

Firewall routes all the traffic in the game so redundant firewall system is needed for this project in case the other one fails. This could be crucial as the game is used as a teaching platform. The scenarios could take time to complete so it is very frustrating for the user (player) to lose all his/her progression in the game.

Cisco ASA supports two types of failover: stateless and stateful. If a failover occurs in stateless failover, all connections that are active at the moment, are dropped and the connection is needed to re-establish again. The stateless failover is the regular failover. Both units use this failover link to communicate and determine the operating status of another unit. (Cisco N.d.e.) The connections which stateless failover passes to the other device, are listed below.

Stateless failover supports:

- Unit state (active/standby)
- Hello-messages (keep-alive)
- Network link status
- MAC-address exchange
- Configuration replication
- Synchronization (Cisco N.d.e.)

In stateful failover the active unit passes connection info continually to the standby unit. The new active unit keeps the same connection alive if failover occurs. If end-user applications are supported by this feature, they are not needed to be reconnected. (Cisco N.d.e.) The connections which stateful failover passes to the other device, are listed below.

Stateful failover supports:

- NAT translation table
- TCP/UDP connection states
- ARP table
- L2 bridge table (in transparent firewall mode)
- HTTP connection state (if HTTP replication is enabled)
- ISAKMP and IPsec SA table
- GTP PDP connection database
- SIP signalling sessions
- ICMP connection state
- Dynamic Routing Protocols (Cisco N.d.e.)

Stateless and stateful failovers can be used with both failover modes: Active/Active and Active/Standby. (Cisco N.d.e.)



Active/Active failover mode can only be used in multiple context mode. Both ASAs pass traffic but security contexts are divided into two failover groups. Failover group is a logical group consisting of one or more security contexts. One group is active on the primary ASA and the other group is active on the secondary ASA. (Cisco N.d.e.)

In Active/Standby failover mode, one unit is active and the second is in standby. Active unit passes traffic and if failover occurs, the active unit goes into standby and the standby unit goes active. Active/Standby can be used in both single and multiple context mode. (Cisco N.d.e.)

More about failover and how it works in chapter 4.11, Failover test.

### 3.6 SSH

Secure Shell is a network protocol to be used in secured remote access. It is mainly used on Linux and Unix based systems but is also available for Windows and Macintosh. SSH provides strong authentication, for example authenticating a user using remote access. In addition, the encryption makes the connection so secure that it is almost impossible for an outsider to hijack the traffic or passwords. With SSH, executing commands or transferring files can be done between local and remote hosts. (IETF 2006.)

### 3.7 RADIUS

RADIUS is an authentication protocol that provides authentication, authorization and accounting management for various network services. An access client (end device, such as computer or laptop) is a device that is needed to access a larger network. These access clients are connected to RADIUS clients (access servers) which provides access to a larger network. RADIUS clients could be for example switch or wireless access point. RADIUS client sends messages to RADIUS server that processes connection requests or accounting messages and sends back RADIUS message response. (Microsoft N.d.)

### 3.8 ASDM

ASDM is a GUI-based appliance manager for Cisco firewalls to be monitored and managed. It is accessed from a browser by using the management IP-

address of the device as www-address. In addition, it uses secure connection (SSL) so https:// is needed. (Cisco N.d.c.)

In this work, ASDM is used to configure access lists as it is much easier than with a console. Screenshots of used configurations are taken from ASDM interface, for example interfaces as seen in figure 3.

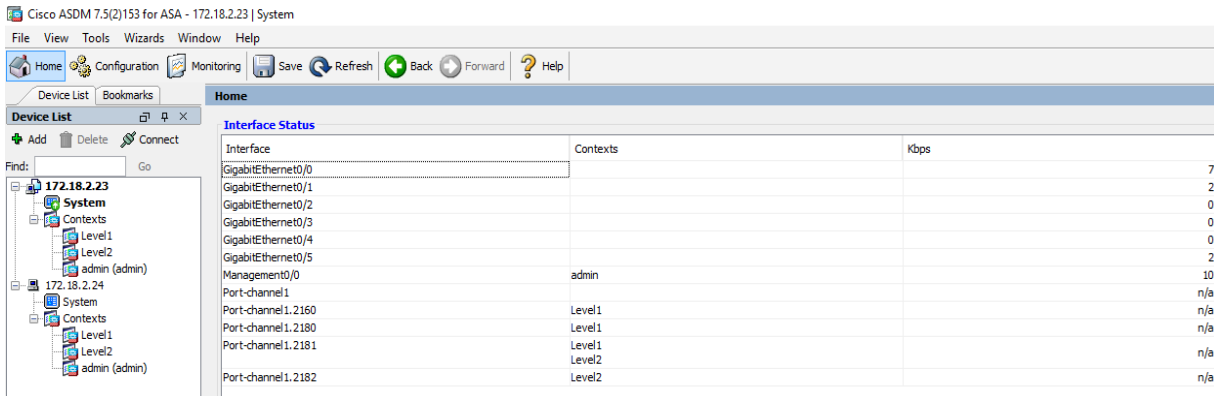


Figure 3. ASDM home menu

### 3.9 NTP

Network Time Protocol is used to synchronize the clocks of computers and devices to a specific time reference. If the clock of one system is ahead of the others, obviously the other systems are behind that. Isolated networks could run on their own time but when the network connects to the Internet, there might be some confusions, like an email from the "future". Without synchronized time all log files are useless as the timestamps do not match. For example billing and financial services. (NTP N.d.b.)

If there is a security breach in the network, it is crucial to have all the devices in the same time. It is much easier to track down the origin of the breach by comparing timestamps in each device's logs, like a trail to follow.

Identity Schemes can be used to identify remote systems. These schemes use encrypted keys between NTP servers (nodes in a large network) and clients to prevent any threats for example man-in-the-middle-attacks. Sequence of NTP servers is called *proventic trail (certificate trail)* which ends at trusted certificate authority. Schemes use only a few bit long keys so the keys should be updated constantly. (NTP N.d.a.) These Identity Schemes are listed below.

Identity Schemes:

- Private Certificate (PC)
- Trusted Certificate (TC)
- Schnorr Identity Scheme (IFF)
- Guillou-Quisquater Identity Scheme (CQ)
- Mu-Varadhajarn Identity Scheme (NTP N.d.a.)

Certificates are used in SSL encryption and if client's clock is out of certificate's time range (not usable yet or has been expired), it cannot validate it and therefore will be denied.

NTP needs some reference clock that sets the true time. All devices in the network associated with NTP server uses the NTP as reference clock. NTP is a UDP based protocol and uses UTC as reference time. (NTP N.d.b.) NTP devices are configured with stratum levels, which are hierarchical. Stratum 0 being the highest and 16 being the lowest. Stratum 1 gets the time from stratum 0, stratum 2 gets the time from stratum 1 and so on. Stratum 0 is a source, for example a satellite (GPS) or an atomic clock.

### 3.10 Tiny Core Linux (OS)

Tiny Core is a very small Linux distribution that has all the basic functions. It can be as small as ten megabytes, which means that it can be stored and run from a storage device. As Tiny Core is very small, it does not come with any software so the users need to install whatever they need. (Tiny Core Team 2007.)

Installing Tiny Core to a hard drive is not the purpose of Tiny Core project. To make the system run fast and protecting the files from changing, it is loaded from a storage device to RAM. This makes sure that on every boot, the system runs properly. This also means that by default, software is installed on RAM, which means that it gets wiped on reboot. (Kasanen 2013.)

Tiny Core Linux is installed and virtualized in Cybergame cluster, thus making it keep all the changes and software installed if for some reason TC shuts down. In this work, Tiny Core Linux is only used for testing a ping from a subnet to another when access lists are configured. Each subnet except man-

agement has its own TCL, which are given an IP-address from their own subnet with last byte being .95. Firewall will be used as a gateway.

## 4 FIREWALL IMPLEMENTATION

### 4.1 Cisco ASA 5515-X

The dimensions (H x W x D) of Cisco ASA 5515-X are 4,24 x 42,9 x 39,5 cm. It is rack-mountable and its size is one rack unit. ASA 5515-X can have 15 000 connections per second and can have up to 100 configured VLANs. (Cisco N.d.b.)

The device has six Gigabit Ethernet ports (1000Base-T) for normal network traffic. It has two ports for management access: one Gigabit Ethernet port and one console port. All of them can be connected with a RJ-45 connector. Additionally, it also has two four pin Hi-Speed USB-A for example, upgrading the flash. (Cisco N.d.b.)

What is important for this work is that the 5515-X has two HA options: Active/Active and Active/Standby of which the latter is used. The default licence also allows 5515-X to run in multiple context mode with two additional contexts in addition to System and Admin contexts. (Cisco N.d.b.) Multiple context mode is used in this work.

### 4.2 Installation and initial configurations

The work started by installing the firewalls (named CG-FW1 and CG-FW2) to the server rack and connecting the power supply to the equipment. Gigabit Ethernet interfaces one and two were connected to DELL switches (named CG-S1 and CG-S2) with SFP coppers as the DELL interfaces are Ten Gigabit Ethernet ports. Secondly, both ASAs were connected together via Gigabit Ethernet interfaces four and five in order to configure the failover later. Third step was to connect both firewalls into a management switch (named CG-MGMT) using the management interface. Physical topology is shown in figure 4.

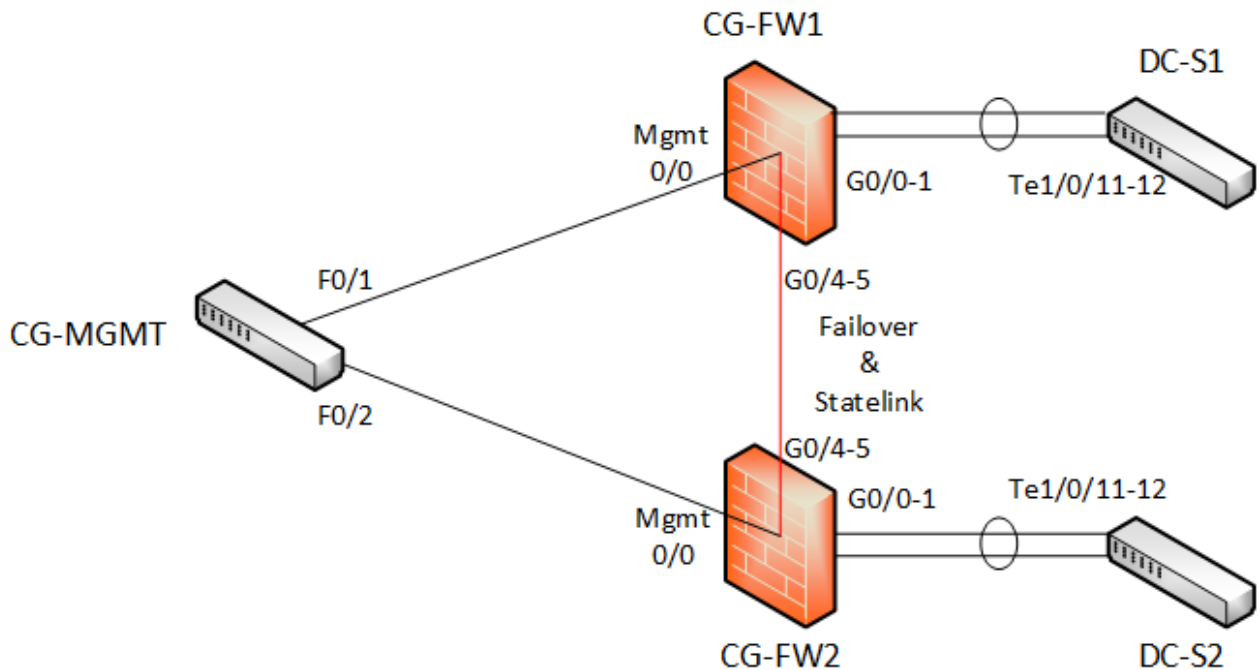


Figure 4. Physical topology

After connecting the cables, a laptop was used to make the remote connection available. Both devices were named and were assigned IP addresses to the management interface: 172.18.2.23 for CG-FW1 and .24 for CG-FW2. At this point it is better to specify the standby management IP to CG-FW1 for the failover configuration later:

```
ip address 172.18.2.23 255.255.255.0 standby 172.18.2.24
```

If the standby management IP is missing when enabling the failover, the secondary unit will not respond as it copies all configurations from the primary unit, like assuming the IP and MAC addresses of the primary unit.

Nameif is by default *management* in the management interface. The remote connection used firewall's local database at first so a local user had to be done with a command *username x password x* in global configuration mode. After creating the user, the remote connection could be set up in global configuration mode:

```
aaa authentication ssh console LOCAL
```

```
crypto key generate rsa modulus 1024
```

```
ssh "internal network" "network mask" management
```

```
ssh version 2
```

At first, this did not work because a static route to the outside network was missing. This was fixed with a command *route management 0 0 172.18.2.1*. Unlike in other Cisco devices, in ASA you need to specify the interface (nameif) in the command.

### 4.3 Logical topology

The ASA 5515-X supports multiple context mode (base license is used) so both additional security contexts, Level1 and Level2, are used as virtual firewalls. Frontend and NEST are the least secure and Management is the most secure. Security levels on Level1 for Frontend/NEST is 0 and for Backend it is 100. On Level2, security levels for Backend is 0 and for Management it is 100. Logical topology of contexts and VLANs is seen in figure 5.

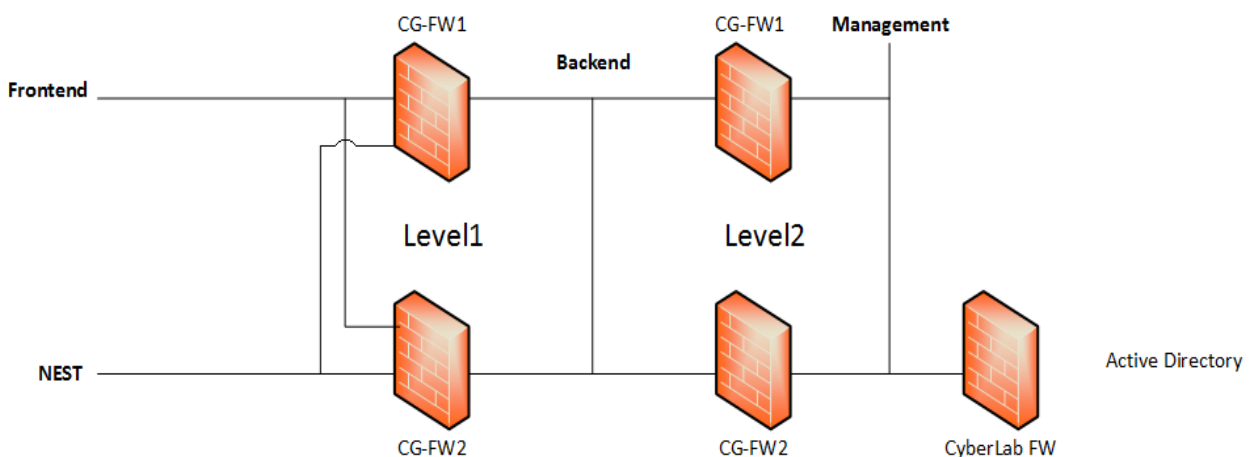


Figure 5. Logical topology

The next phase was to set both firewalls into multiple context mode. Input the command *mode multiple* in global configuration mode. After inputting the command, devices were reloaded and both booted up with system, admin and two additional security contexts. Switching between contexts is done by using command *changeto context contextname*. Switching to system context is done by inputting *changeto system*. Both of these commands are used in privileged EXEC Mode.

#### 4.4 Failover configuration

To make both firewalls redundant, failover was next on the list. CG-FW1 will act as a primary unit and CG-FW2 will act as a secondary unit. Failover configuration is done in system context in global configuration mode. LAN failover-link is named *folink* and a subnet used for failover-link is 172.18.4.0 /24.

These commands are inputted in CG-FW1:

```
failover lan unit primary
```

```
failover lan interface folink g0/4
```

```
failover lan interface ip folink 172.18.4.1 255.255.255.0 standby 172.18.4.2
```

The first command tells the unit which one it will be, primary or secondary.

The second command specifies the name of the failover-link and which physical interface it uses. The third command specifies the failover IP addresses of the active unit and the standby unit. The same commands were used in CG-FW2 but with only changing the *primary* to *secondary*.

After setting the LAN failover -link commands, it was necessary to make the protocol functional. First task to do was to use *no shutdown* command for g0/4 interfaces in both devices in order to get the physical link up. Then using the command *failover* in both devices in global configuration mode enables the failover and makes the protocol working as intended.

From now on, configuring only the active unit is needed because the standby unit copies all configurations from the active unit. Configuring the standby unit will not replicate any configurations to the active unit. To force the standby unit to go into active mode, use the command *failover active* in global configuration mode in system context.

As the idea of implementing the Stateful failover came up later, it was configured in ASDM interface. Stateful failover was given a subnet 172.18.5.0 /24 and was named *statelink*. Both failovers can use the same interface but as there were no use for remaining interfaces, interface g0/5 was dedicated to *statelink*. This also load balances the traffic as both failovers have their own dedicated link. Configurations of both failovers can be seen in figure 6.

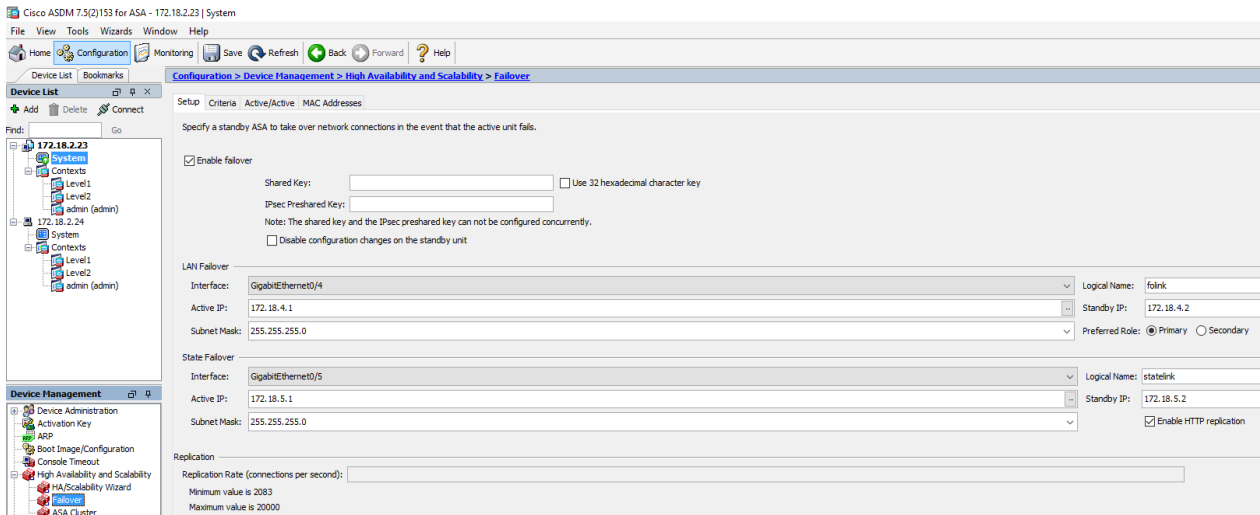


Figure 6. LAN Failover and State Failover in ASDM UI

## 4.5 LACP configuration

Next phase was to configure LACP, which is configured in system context. Gigabit interfaces 0/1 and 0/2 were bundled together (as can be seen in figures 4 or 8) and all the VLANs were assigned to that bundle link. The following commands were used to create the port-channel with LACP:

```
interface gigabitethernet0/1
description DC-SX_Te1/0/11
channel-group 1 mode active
```

The same commands were applied to G0/2 but in the description 11 was replaced with 12. To assign VLANs to the port-channel, they were created as sub-interfaces with the following commands:

```
interface Port-channel1.2160
description NEST
```

The same commands were used with other VLANs (Frontend, Backend and Management) but sub-interface "ID" and description were replaced with the ones assigned to them.



## 4.6 Context configurations

When the LACP port-channel was configured, virtual firewalls (Level1 and Level2) were configured. As you can see from figures 5 and 8: Level1 manages traffic in Nest, Frontend and Backend; Level2 manages traffic in Backend and Management. Contexts were created in system in global configuration mode with the following commands:

*context Level1* and for Level2, *context Level2*.

When the context was created, sub-interfaces and VLANs were then needed to assign to proper contexts so they know which virtual firewall to use. These configurations (Level1 as an example) were applied with the following commands:

*allocate-interface Port-channel1.2160 vlan2160*

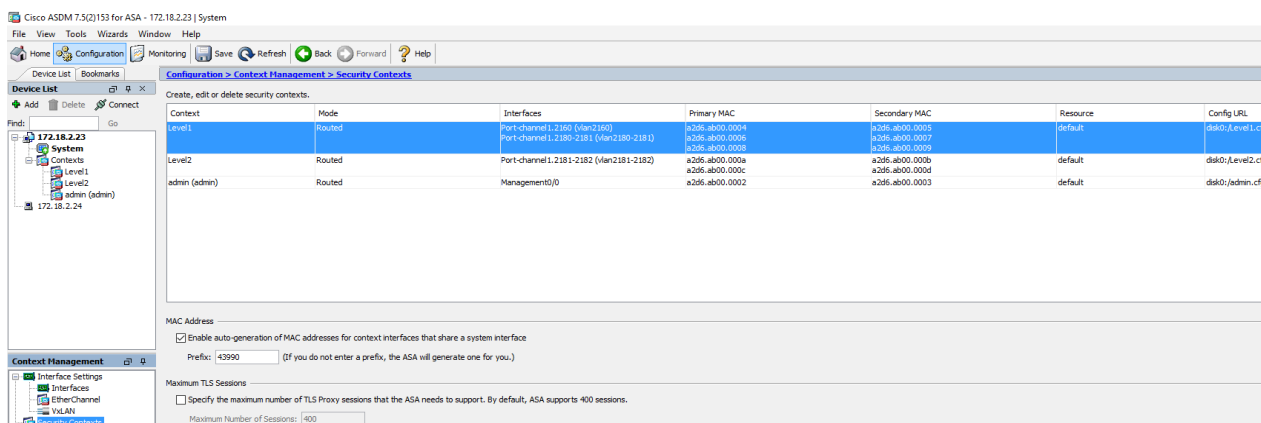
*allocate-interface Port-channel1.2180-2181 vlan2180-vlan2181*

Also for the context configuration to be stored into the system in boot, the following command needed to be applied:

*config-url disk0:/Level1.cfg*

See figure 7 for created security contexts seen from ASDM UI.

Cisco configuration guide states that the *config-url* command has to be inputted last because it will save all its context configurations before that. If the command is inputted first, the system will load (for example in reboot) the context but will not load any of the configurations like allocated interfaces. (Cisco N.d.d.)



Context	Mode	Interfaces	Primary MAC	Secondary MAC	Resource	Config URL
Level1	Routed	Port-channel1.2160 (Vlan2160) Port-channel1.2180-2181 (Vlan2180-2181)	a206.ab00.0004 a206.ab00.0006 a206.ab00.0008	a206.ab00.0005 a206.ab00.0007 a206.ab00.0009	default	disk0:/Level1.cfg
Level2	Routed	Port-channel1.2181-2182 (Vlan2181-2182)	a206.ab00.000a a206.ab00.000c	a206.ab00.000b a206.ab00.000d	default	disk0:/Level2.cfg
admin (admin)	Routed	Management/0	a206.ab00.0002	a206.ab00.0003	default	disk0:/admin.cfg

MAC Address

Enable auto-generation of MAC addresses for context interfaces that share a system interface

Prefix: 43990 (If you do not enter a prefix, the ASA will generate one for you.)

Maximum TLS Sessions

Specify the maximum number of TLS Proxy sessions that the ASA needs to support. By default, ASA supports 400 sessions.

Maximum Number of Sessions: 400

Figure 7. Security contexts in ASDM UI.

Final addition to context configurations was the IP addressing of the contexts or more likely, VLANs in this case. For each VLAN IP address, last byte was .5 for active and .6 for standby. The only exception was Backend on Level2. Backend works as an interface between Level1 and Level2 and therefore cannot use the same IP addressing on both. For Level2 context, Backend was allocated with .1 and .2. At this point security levels are also configured with the values said earlier. Configuring NEST on context Level1 as an example:

```
interface vlan2160
```

```
nameif NEST
```

```
security-level 0
```

```
ip address 172.16.0.5 255.255.0.0 standby 172.16.0.6
```

After Level1 interfaces had been given an IP address, nameif and security level, Level2 was switched and configured like the same. See figure 8 for allocated sub-interfaces.

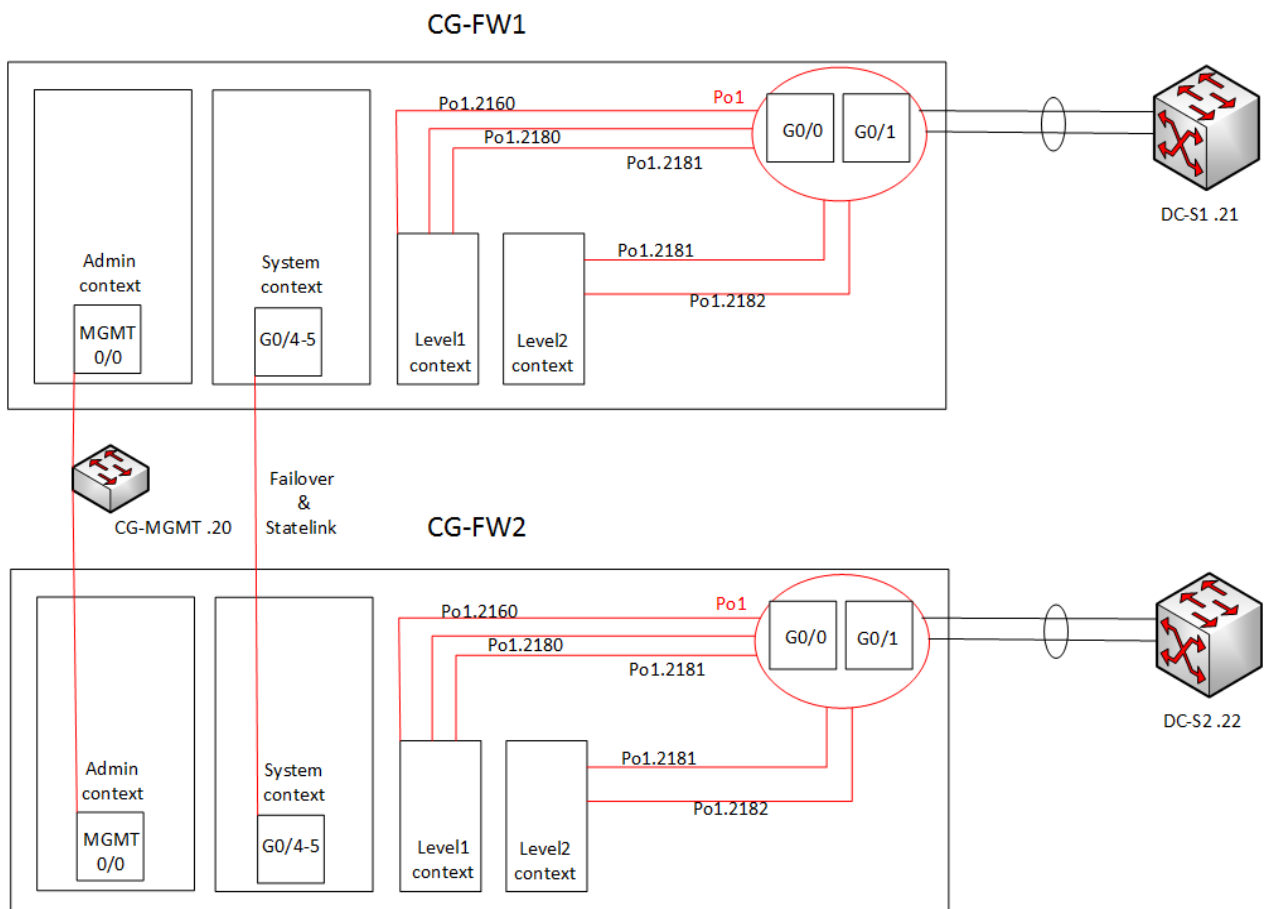


Figure 8. Physical connections and sub-interfaces to contexts

## 4.7 ASDM

The configuration is very similar to SSH and to allow ASDM be used in firewalls, the following commands are needed:

```
http server enable
```

```
http "internal network" "network mask" management
```

```
aaa authentication http console LOCAL
```

## 4.8 Protocol configurations

In this chapter various protocols are configured. These protocols are merely a slight addition to the work and are configured in admin context except NTP that is configured in system context.

### 4.8.1 NTP

Four of Funet's NTP servers were used in this work, which are used in most Finnish universities. Like in previous protocols, also in NTP's configuration commands the interface were specified and the "prefer" at the end is somewhat self-explanatory. See figure 9 for NTP configuration with ASDM and figure 10 for NTP status.

```
ntp authenticate
```

```
ntp server 193.166.5.197 source management prefer
```

```
ntp server 193.166.5.207 source management
```

```
ntp server 193.166.5.177 source management
```

```
ntp server 193.166.5.217 source management
```

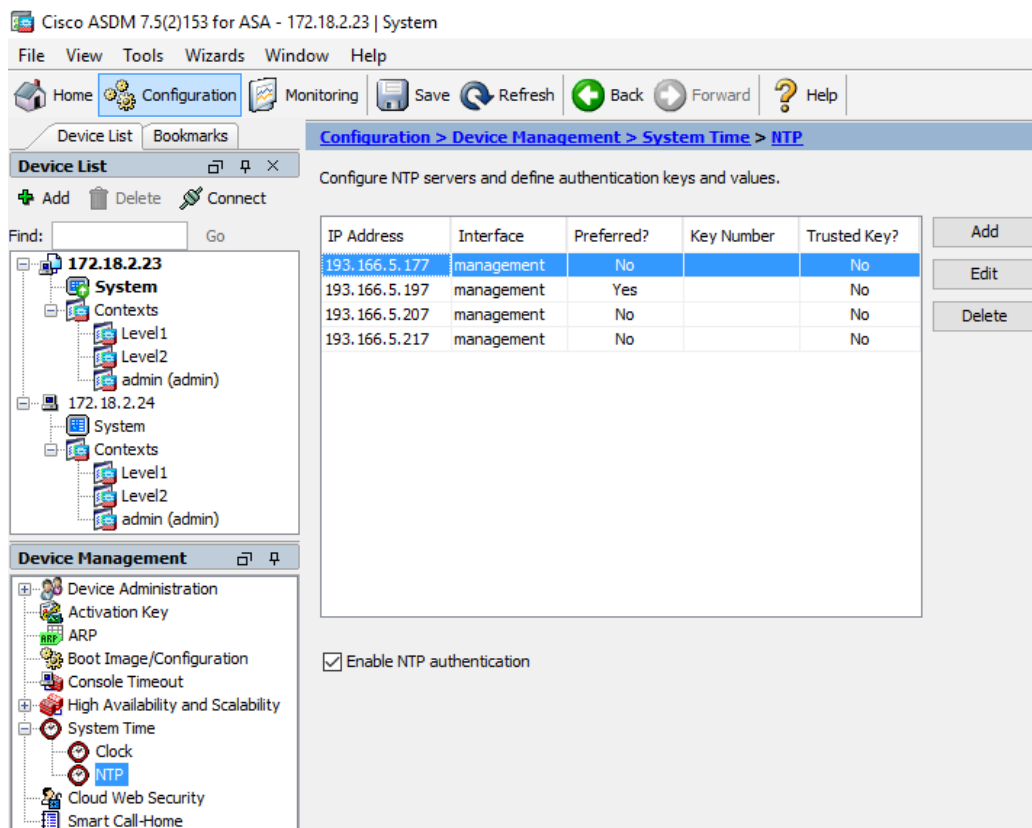


Figure 9. NTP configuration in ASDM UI

```
CG-FW1/pri/act# show ntp status
Clock is synchronized, stratum 2, reference is 193.166.5.197
nominal freq is 99.9984 Hz, actual freq is 99.9925 Hz, precision is 2**6
reference time is dca453a1.6a9bb7bb (09:47:13.416 UTC Fri Apr 21 2017)
clock offset is -0.5910 msec, root delay is 7.13 msec
root dispersion is 17.33 msec, peer dispersion is 15.75 msec
CG-FW1/pri/act# show ntp assoc
      address      ref clock   st  when  poll reach  delay  offset  disp
*~193.166.5.197   .MRS.      1   254  1024  377    7.1   -0.59  15.7
+~193.166.5.207   .MRS.      1   304  1024  377   15.5  -0.13  15.9
+~193.166.5.177   .MRS.      1   321  1024  377    7.9   -0.44  15.7
+~193.166.5.217   .MRS.      1   377  1024  377   14.7  -0.51  15.7
 * master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
CG-FW1/pri/act#
```

Figure 10. NTP status and associates

#### 4.8.2 RADIUS

When RADIUS privileges were configured in the server for the firewalls, the remote console access as local user could be removed, as it was a security risk. First, the firewalls were configured to use RADIUS protocol with a server-group named RADIUS:

```
aaa-server RADIUS protocol radius
```

```
aaa-server RADIUS (management) host "server IP"
```

```
key xxx
```

The second command specifies the interface the device is using and the RADIUS-server IP-address. The third command is the RADIUS-key that is given from the server. Firewalls can be configured to use multiple RADIUS-servers in case one fails.

Both SSH and ASDM were then configured to use RADIUS instead of a local database. First, the local database authentication was removed from both and RADIUS authentication was added instead:

```
no aaa authentication ssh console LOCAL
```

```
no aaa authentication http console LOCAL
```

```
aaa authentication ssh console RADIUS
```

```
aaa authentication http console RADIUS
```

If RADIUS-servers are down for some reason, a local user was still kept but only restricted to a local console access as seen in figures 11 and 12.

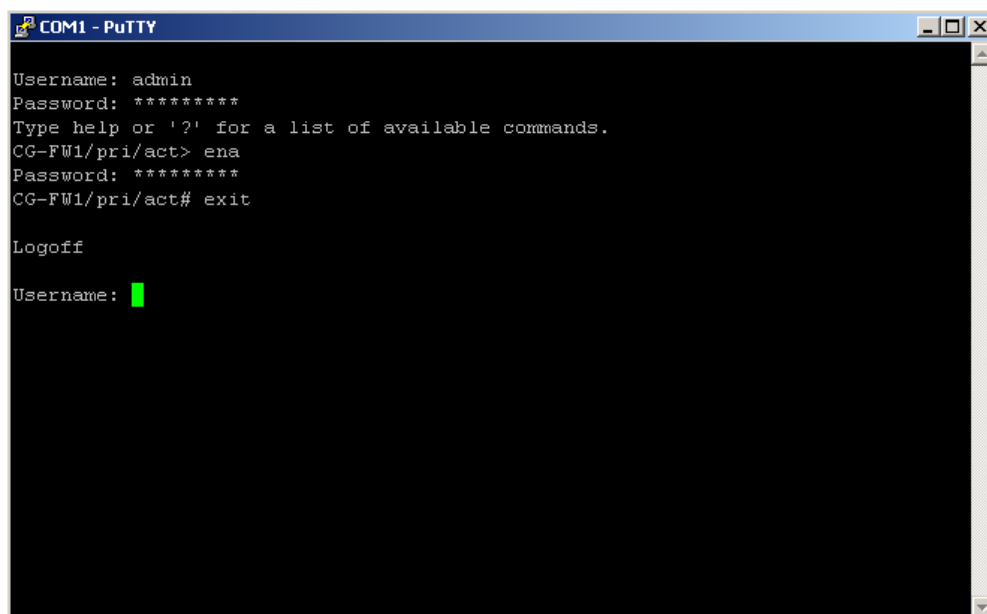
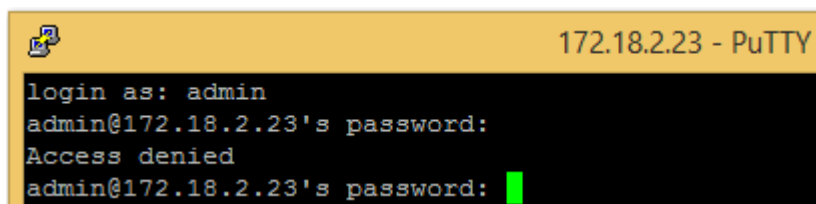


Figure 11. Local console access

A screenshot of a PuTTY terminal window. The title bar at the top right reads "172.18.2.23 - PuTTY". The terminal content shows a login prompt "login as: admin", followed by "admin@172.18.2.23's password:", then "Access denied", and finally "admin@172.18.2.23's password:" with a green cursor at the end.

```
login as: admin
admin@172.18.2.23's password:
Access denied
admin@172.18.2.23's password: █
```

Figure 12. Remote access with admin user

### 4.8.3 Syslog

Message logging was needed in the firewalls for them to send informational messages to already existing syslog-server. In the work, the messages are timestamped and shows which users have accessed (by default they are hidden) to the firewalls and which configurations they have made (if any). In Cybergame design, firewalls were given local1 as identification, which means that facility code is 17. There are numerous options for logging as seen in figure 13. See figure 14 how syslog-messages are shown in the server. The following commands enable the logging to the server using the management-interface:

*logging enable*

*logging timestamp*

*no logging hide username*

*logging facility 17*

*logging host management "server IP"*

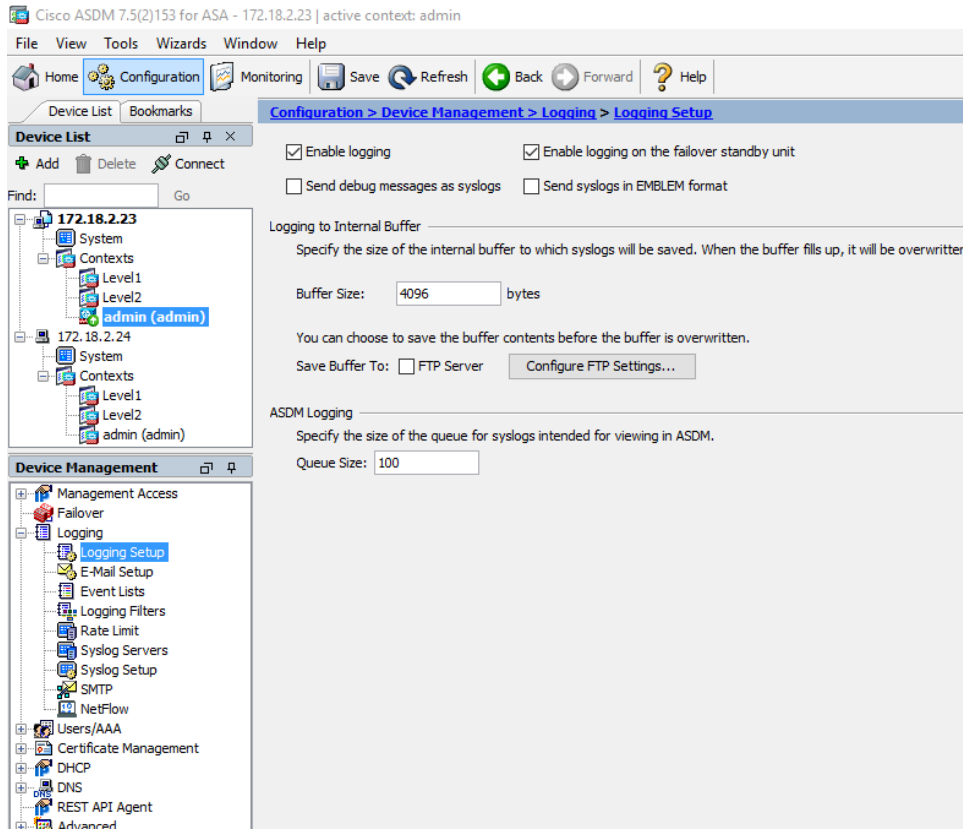


Figure 13. Syslog and its sub-categories in ASDM UI

Today 09:58:14	LOCAL1	NOTICE	172.18.2.23	%ASA-5-111010:	Syslog	User 'asko.hakkarainen', running 'N/A' from IP 10.69.34.103, executed 'write me ...
Today 09:58:14	LOCAL1	NOTICE	172.18.2.23	%ASA-5-111008:	Syslog	User 'asko.hakkarainen' executed the 'write memory' command.
Today 09:58:14	LOCAL1	NOTICE	172.18.2.23	%ASA-5-111004:	Syslog	console end configuration: OK
Today 09:58:14	LOCAL1	NOTICE	172.18.2.23	%ASA-5-111001:	Syslog	Begin configuration: console writing to memory
Today 09:58:14	LOCAL1	NOTICE	172.18.2.23	%ASA-5-111007:	Syslog	Begin configuration: 10.69.34.103 reading from http [POST]
Today 09:58:14	LOCAL1	INFO	172.18.2.23	%ASA-6-605005:	Syslog	Login permitted from 10.69.34.103/56744 to management:172.18.2.23/https for use ...

Figure 14. Syslog-messages in the server.

#### 4.9 PVLAN configuration

In Cisco ASA devices, the PVLANS are considered secondary VLANs as seen in figure 15. Traffic received on the secondary VLAN will be redirected to the primary VLAN. PVLANS (VLAN NEST as a reference) were configured to sub-interfaces in system context with the following commands:

```
interface Port-channel1.2160
```

```
vlan 2160 secondary 2260
```

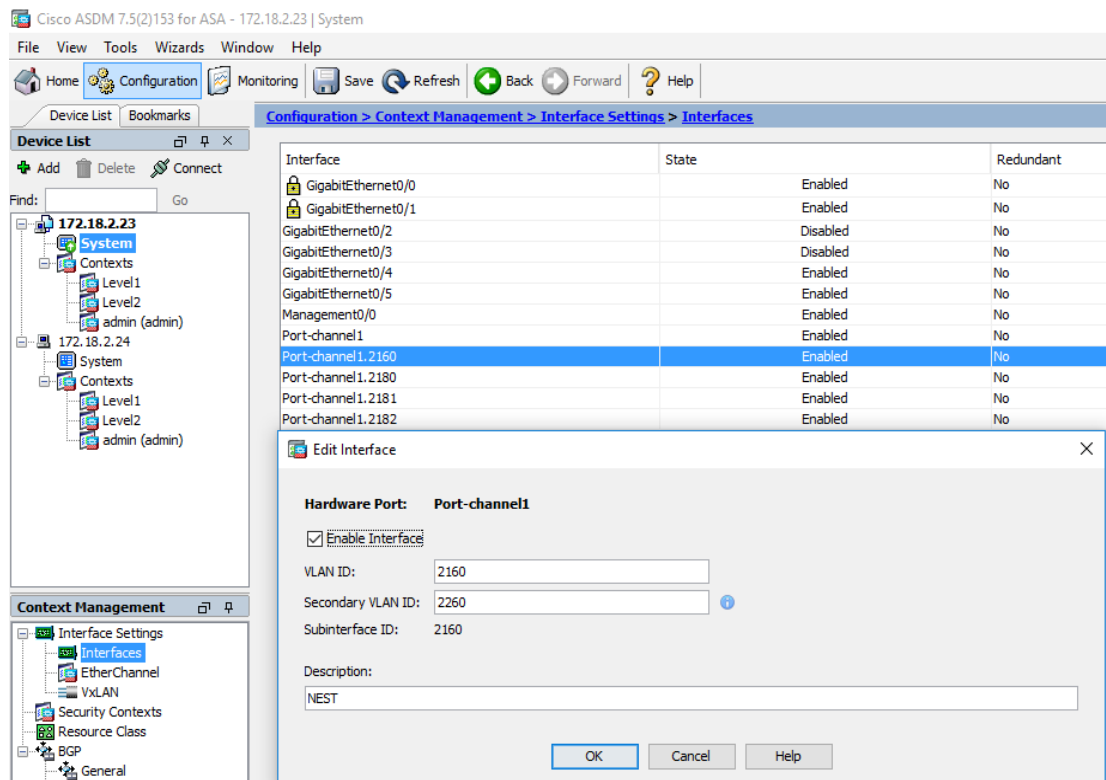


Figure 15. Secondary VLAN configuration in ASDM UI

## 4.10 ACLs

By default, the global implicit rule in firewalls denies all traffic to whatever direction. Then comes the implicit rule for security levels where traffic from a lower security level interface to a higher security level interface will also be blocked. To bypass these implicit rules, access lists are needed. In this work, the interfaces in need of access lists are Frontend and NEST on Level1 and Backend on Level2. See figure 18 for implicit rules.

For testing purposes only, all IP traffic is permitted. The first sub-chapter is about testing the access-lists with ICMP ping to see they work. The second sub-chapter is about how to monitor the traffic and to see which type of traffic should be permitted with access lists.

### 4.10.1 Creating and testing access lists

The ACLs were configured in context's firewall in ACL manager by clicking the *Add* and then *Add ACL* button. On Level1 the access lists were given names *FE->* and *NEST->* and on Level2 the ACL was named *BE->*. These ACLs are empty so in order for them to work, rules are needed to filter the traffic by se-



lecting the ACL and clicking *Add* and then *Add ACE*. See figure 16 for created access lists with rules.

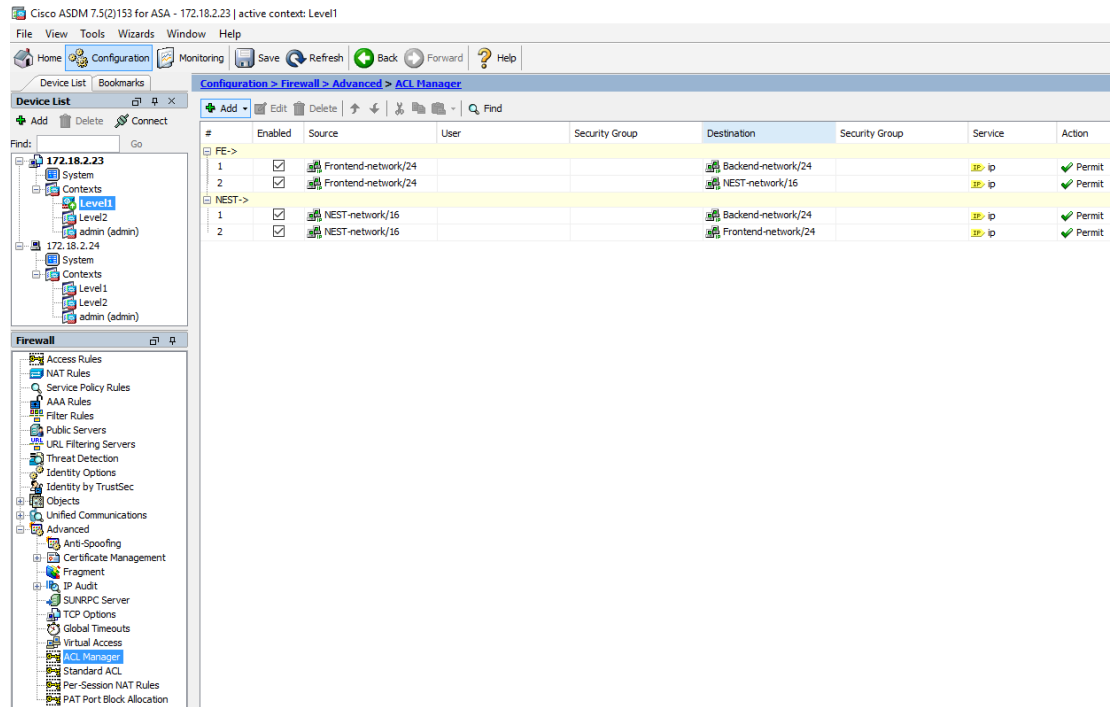


Figure 16. Frontend and NEST ACLs on Level1

After adding the rules to the ACLs, Tiny Core Linuxes were needed to verify that traffic would not be denied from subnet to another. Pings are successful on Level1 as seen in figures 17 and 18.

```

Terminal
tc@box:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:8B:20:C4
          inet addr:172.16.0.95  Bcast:172.16.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:62054982  errors:0  dropped:224  overruns:0  frame:0
          TX packets:2763  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:3475090400 (3.2 GiB)  TX bytes:171714 (167.6 KiB)

tc@box:~$ ping 172.18.0.95 -c 4
PING 172.18.0.95 (172.18.0.95): 56 data bytes
64 bytes from 172.18.0.95: seq=0 ttl=64 time=0.890 ms
64 bytes from 172.18.0.95: seq=1 ttl=64 time=0.707 ms
64 bytes from 172.18.0.95: seq=2 ttl=64 time=0.824 ms
64 bytes from 172.18.0.95: seq=3 ttl=64 time=1.011 ms

--- 172.18.0.95 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.707/0.858/1.011 ms
tc@box:~$ ping 172.18.1.95 -c 4
PING 172.18.1.95 (172.18.1.95): 56 data bytes
64 bytes from 172.18.1.95: seq=0 ttl=64 time=0.998 ms
64 bytes from 172.18.1.95: seq=1 ttl=64 time=0.846 ms
64 bytes from 172.18.1.95: seq=2 ttl=64 time=0.822 ms
64 bytes from 172.18.1.95: seq=3 ttl=64 time=0.788 ms

--- 172.18.1.95 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.788/0.863/0.998 ms
tc@box:~$

```

Figure 17. Pings from a subnet NEST to Frontend and Backend

#	Enabled	Source Criteria	Destination Criteria	Service	Action	Hits	Logging	Time	Description
1		any	Any less secure networks	ip	Permit				Implicit rule: Permit all traffic to less secure networks
Backend (1 implicit incoming rule)									
1		Frontend-network/24	Backend-network/24	ip	Permit	0			
2		Frontend-network/24	NEST-network/16	ip	Permit	0			
Frontend (2 incoming rules)									
NEST (2 incoming rules)									
1		NEST-network/16	Backend-network/24	ip	Permit	8			
2		NEST-network/16	Frontend-network/24	ip	Permit	8			
Global (1 implicit rule)									
1		any	any	ip	Deny				Implicit rule

Figure 18. ACL rules and ping hits

#### 4.10.2 Monitoring traffic

In Cybergame, we do not know which type of traffic there would be going so permitting all IP traffic was necessary. All traffic between subnets will be logged into a firewall's log buffer. *Log buffer* can be accessed from *Monitoring* tab.

Two devices were needed: a www- and SSH-server and a client what is used to connect the server. Server was installed in Frontend and client was installed in NEST. Both devices were given an IP-address from their own subnet with last byte being .96. In figures 19 and 20, the client has established connection with the server.

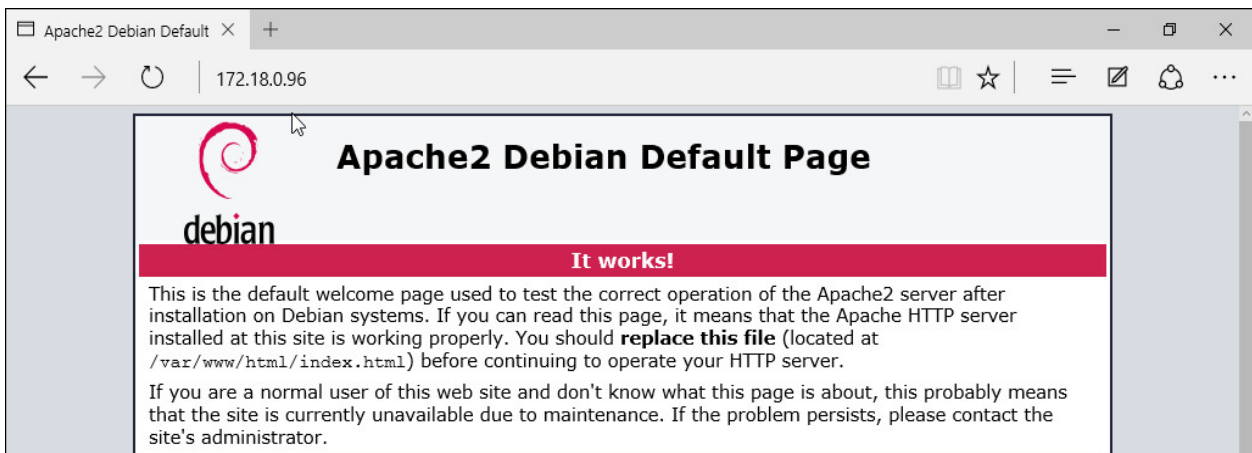


Figure 19. Apache default page seen from the client

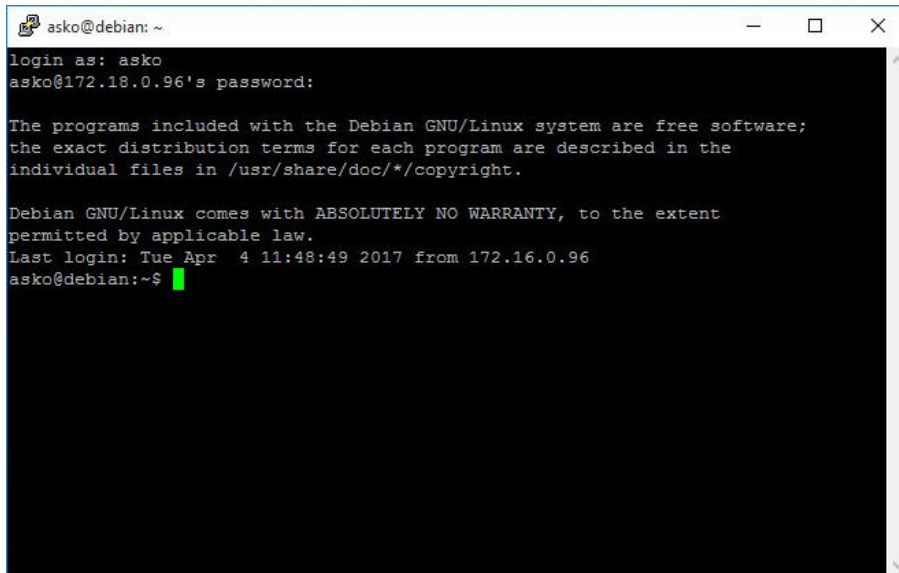


Figure 20. SSH connection established by the client

In this test, the traffic types are known so it was easier to find them in the log. As can be seen in figure 21, TCP connections with ports 22 and 80 from NEST to Frontend have been established. Timestamps are not synchronized (figures 20 and 21) as the server nor the client were configured with NTP. Next phase is to create access lists (figure 23) for http- and SSH-traffic and deleting the "permit all IP traffic".

6	Apr 04 2017	09:01:20	302013	172.16.0.96	49422	172.18.0.96	22	Built inbound TCP connection 18069 for NEST:172.16.0.96/49422 (172.16.0.96/49422) to Frontend:172.18.0.96/22 (172.18.0.96/22)
6	Apr 04 2017	09:01:15	302014	172.16.0.96	49421	172.18.0.96	80	Tear down TCP connection 18064 for NEST:172.16.0.96/49421 to Frontend:172.18.0.96/80 duration 0:01:09 bytes 763 TCP FINs

Figure 21. Log buffer in Cisco ASA

NEST (5 incoming rules)								
4	<input type="checkbox"/>	NEST-network/16		Backend-network/24	IP	IP	Permit	0
2	<input type="checkbox"/>	NEST-network/16		Frontend-network/24	IP	IP	Permit	0
3	<input checked="" type="checkbox"/>	NEST-network/16		Frontend-network/24	TCP	ssh	Permit	1
4	<input checked="" type="checkbox"/>	NEST-network/16		Frontend-network/24	TCP	http	Permit	1
5	<input checked="" type="checkbox"/>	NEST-network/16		Frontend-network/24	ICMP	icmp	Permit	0

Figure 22. New access lists

#### 4.11 Failover test

A small test was conducted to see if the failover works by reloading the primary/active unit. Continuous ping without any parameters was sent from workstation to the primary/active firewall's management address before reloading it. During that reload, three packets were dropped before ping reply was received. Approximately five seconds downtime before the secondary/standby unit assumed the active role and its IP address 172.18.2.23

(Figure 23). During the reload, the IP address 172.18.2.24 was no more available and did not reply to ping.

Cisco guide states that the standby unit assumes both IP and MAC addresses of the primary unit and begins the traffic passing. The former active unit is now in standby state and assumes IP and MAC address of the former standby unit. Devices in the network see no change in IP or MAC address table which means that no ARP entries change or no timeouts occur anywhere. (Cisco N.d.e.)

If both devices boot up at the same time, the primary unit will assume the active role. If the secondary device do not detect the primary device in boot, it will act as the active unit using its own MAC address, as it does not know the MAC address of the primary unit. When primary unit becomes available, the secondary (active) unit takes the MAC address of the primary unit which can cause error in the network as there are two devices with the same MAC address. This can be avoided by generating virtual MAC addresses as seen in the figure 7. (Cisco N.d.e.)

```

172.18.23 - PuTTY
State          Last Failure Reason  Date/Time
This host -    Secondary          None
              Active
Other host -   Primary           Comm Failure      12:25:47 UTC Mar 7 2017

====Configuration State====
Sync Done
Sync Done - STANDBY
====Communication State====

CG-FW1/sec/act# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: folink GigabitEthernet0/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 6 of 114 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.5(2), Mate 9.5(2)
Last Failover at: 12:25:47 UTC Mar 7 2017
This host: Secondary - Active
Active time: 69 (sec)
slot 0: ASAS515 hw/sw rev (1.0/9.5(2)) status (Up Sys)
admin Interface management (172.18.2.23): Normal (Waiting)
Level2 Interface Backend (172.18.1.1): Normal (Waiting)
Level2 Interface MGMT (172.18.2.5): Normal (Waiting)
Level1 Interface NEST (172.16.0.5): Normal (Waiting)
Level1 Interface Frontend (172.18.0.5): Normal (Waiting)
Level1 Interface Backend (172.18.1.3): Normal (Waiting)
slot 1: SFR5515 hw/sw rev (N/A/5.3.1-152) status (Up/Up)
ASA FirePOWER, 5.3.1-152, Up, (Monitored)
Other host: Primary - Failed
Active time: 1636096 (sec)
slot 0: ASAS515 hw/sw rev (1.0/9.5(2)) status (Unknown/Unknown)
admin Interface management (172.18.2.24): Unknown (Monitored)
Level2 Interface Backend (172.18.1.2): Unknown (Monitored)
Level2 Interface MGMT (172.18.2.6): Unknown (Monitored)
Level1 Interface NEST (172.16.0.6): Unknown (Monitored)
Level1 Interface Frontend (172.18.0.6): Unknown (Monitored)
Level1 Interface Backend (172.18.1.6): Unknown (Monitored)
slot 1: SFR5515 hw/sw rev (N/A/5.3.1-152) status (Unknown/Unknw
ASA FirePOWER, 5.3.1-152, Unknown, (Monitored)

Stateful Failover Logical Update Statistics
Link : statelink GigabitEthernet0/5 (up)
Stateful Obj  xmit      xerr      rcv      rerr
General        1622      0          1722     0
sys cmd        1622      0          1621     0
up time        0          0           0         0
RPC services   0          0           0         0
TCP conn       0          0           0         0
UDP conn       0          0           0         0
ARP tbl        0          0           98         0
Xlate Timeout  0          0           0         0
IPv6 ND tbl    0          0           0         0
VPN IKEv1 SA   0          0           0         0
VPN IKEv1 P2   0          0           0         0
VPN IKEv2 SA   0          0           0         0
VPN IKEv2 P2   0          0           0         0
VPN CTCP upd   0          0           0         0
VPN SDI upd    0          0           0         0
VPN DHCP upd   0          0           0         0
SIP Session    0          0           0         0
SIP Tx 0       0          0           0         0
SIP Pinhole    0          0           0         0
Route Session  0          0           0         0
Router ID      0          0           0         0
User-Identity  0          0           3         0
CTS SGTNAME    0          0           0         0
CTS PAC        0          0           0         0
TrustSec-SXP   0          0           0         0
IPv6 Route     0          0           0         0
STS Table      0          0           0         0

Logical Update Queue Information
Cur  Max  Total
Recv Q: 0  21  39530
Xmit Q: 0  1  1622

CG-FW1/sec/act# Beginning configuration replication: Sending to mate.
End Configuration Replication to mate.

172.18.24 - PuTTY
CG-FW1/pri/stby# show failover state
State          Last Failure Reason  Date/Time
This host -    Primary           None
              Standby Ready
Other host -   Secondary          Active

====Configuration State====
Sync Done - STANDBY
====Communication State====
Mac set

CG-FW1/pri/stby# show failover
Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 6 of 114 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.5(2), Mate 9.5(2)
Last Failover at: 12:27:40 UTC Mar 7 2017
This host: Primary - Standby Ready
Active time: 0 (sec)
slot 0: ASAS515 hw/sw rev (1.0/9.5(2)) status (Up Sys)
admin Interface management (172.18.2.24): Normal (Waiting)
Level2 Interface Backend (172.18.1.2): Normal (Waiting)
Level2 Interface MGMT (172.18.2.6): Normal (Waiting)
Level1 Interface NEST (172.16.0.6): Normal (Waiting)
Level1 Interface Frontend (172.18.0.6): Normal (Waiting)
Level1 Interface Backend (172.18.1.6): Normal (Waiting)
slot 1: SFR5515 hw/sw rev (N/A/) status (Init/Up)
Other host: Secondary - Active
Active time: 161 (sec)
slot 0: ASAS515 hw/sw rev (1.0/9.5(2)) status (Up Sys)
admin Interface management (172.18.2.23): Normal (Waiting)
Level2 Interface Backend (172.18.1.1): Normal (Waiting)
Level2 Interface MGMT (172.18.2.5): Normal (Waiting)
Level1 Interface NEST (172.16.0.5): Normal (Waiting)
Level1 Interface Frontend (172.18.0.5): Normal (Waiting)
Level1 Interface Backend (172.18.1.3): Normal (Waiting)
slot 1: SFR5515 hw/sw rev (N/A/5.3.1-152) status (Up/Up)
ASA FirePOWER, 5.3.1-152, Up, (Monitored)

Stateful Failover Logical Update Statistics
Link : statelink GigabitEthernet0/5 (up)
Stateful Obj  xmit      xerr      rcv      rerr
General        4          0           29         0
sys cmd        4          0           4         0
up time        0          0           0         0
RPC services   0          0           0         0
TCP conn       0          0           0         0
UDP conn       0          0           0         0
ARP tbl        0          0           22         0
Xlate Timeout  0          0           0         0
IPv6 ND tbl    0          0           0         0
VPN IKEv1 SA   0          0           0         0
VPN IKEv1 P2   0          0           0         0
VPN IKEv2 SA   0          0           0         0
VPN IKEv2 P2   0          0           0         0
VPN CTCP upd   0          0           0         0
VPN SDI upd    0          0           0         0
VPN DHCP upd   0          0           0         0
SIP Session    0          0           0         0
SIP Tx 0       0          0           0         0
SIP Pinhole    0          0           0         0
Route Session  0          0           0         0
Router ID      0          0           0         0
User-Identity  0          0           3         0
CTS SGTNAME    0          0           0         0
CTS PAC        0          0           0         0
TrustSec-SXP   0          0           0         0
IPv6 Route     0          0           0         0
STS Table      0          0           0         0

Logical Update Queue Information
Cur  Max  Total
Recv Q: 0  14  169
Xmit Q: 0  1  4

CG-FW1/pri/stby#

```

Figure 23. Secondary unit as an active unit and primary unit as a standby unit.

By looking at the “last failover at” in figure 23, it took two minutes before the former active unit was done with reloading and assumed the standby role and its IP address 172.18.2.24. Failover works as intended and the primary/standby unit was forced to be active again (figure 24).

```
CG-FW1/pri/act# show failover history
```

From State	To State	Reason
12:27:47 UTC Mar 7 2017 Not Detected	Negotiation	No Error
12:27:51 UTC Mar 7 2017 Negotiation	Cold Standby	Detected an Active mate
12:27:52 UTC Mar 7 2017 Cold Standby	Sync Config	Detected an Active mate
12:28:01 UTC Mar 7 2017 Sync Config	Sync File System	Detected an Active mate
12:28:01 UTC Mar 7 2017 Sync File System	Bulk Sync	Detected an Active mate
12:28:14 UTC Mar 7 2017 Bulk Sync	Standby Ready	Detected an Active mate
12:31:54 UTC Mar 7 2017 Standby Ready	Just Active	Set by the config command
12:31:54 UTC Mar 7 2017 Just Active	Active Drain	Set by the config command
12:31:54 UTC Mar 7 2017 Active Drain	Active Applying Config	Set by the config command
12:31:54 UTC Mar 7 2017 Active Applying Config	Active Config Applied	Set by the config command
12:31:54 UTC Mar 7 2017 Active Config Applied	Active	Set by the config command

Figure 24. Primary unit as an active unit again with failover history shown

In other words, the North-South firewall is not redundant for at least two minutes as the former active unit boots up. The downtime for redundancy could be more if for example, the active unit's input power is interrupted or failover link fails for some reason.

## 5 CONCLUSION

The work was completed to the point where Cybergame needed it to be as the game itself was not ready. The access lists are at the moment in "permit any" state and are needed to change. As Cybergame is not finished, there is no traffic between VLANs or security contexts to know what traffic types will be permitted or denied. If detailed access lists are not factored in, the work can be considered as complete.

Even though this work was part of Cybergame project, there was only a little communication with others who worked on the project as it did not seem to have an impact on the work. Only PVLAN configuration was done in collaboration with someone working on a virtualization in Cybergame. That was as the

"someone" needed to check traffic between VMs in different PVLANS but to redirect the traffic, PVLANS were needed to configure in the firewall as it routes the traffic inside.

The work itself was at first interesting and challenging as there was only a little experience with Cisco firewalls. Especially with the 5515-X model (that was used in the work) since the previous experience was with 5505 model. A lot of knowledge was gained about Cisco 5515-X but many features were left uncovered.

If Cybergame will be finished one day, the infrastructure for it will be almost ready. Maybe someone will work on the firewall(s) as a project (for thesis work there will not be much to do) and make proper access-lists or implement new ideas if needed.

## REFERENCES

- Cisco. N.d.a. Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE. Available at: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2\\_25\\_see/configuration/guide/scg/swpvlan.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_25_see/configuration/guide/scg/swpvlan.html) [Accessed 15 November 2016].
- Cisco. N.d.b. Cisco ASA 5515-X Adaptive Security Appliance. Available at: <http://www.cisco.com/c/en/us/support/security/asa-5515-x-adaptive-security-appliance/model.html> [Accessed 8 November 2016].
- Cisco. N.d.c. Cisco Adaptive Security Device Manager. Available at: <http://www.cisco.com/c/en/us/products/security/adaptive-security-device-manager/index.html> [Accessed 17 January 2017].
- Cisco. N.d.d. CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.2. Available at: <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ha-contexts.html> [Accessed 3 January 2017].
- Cisco. N.d.e. CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.2. Available at: <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ha-failover.html> [Accessed 21 March 2017].
- Euroopan aluekehitysräho. 2014. Available at: <https://www.eura2014.fi/rrtiepa/projekti.php?projektiid=A70554> [Accessed 25 October 2016].
- IEEE Standards Association. 2001. IEEE P802.3ad. Available at: <http://grouper.ieee.org/groups/802/3/ad/index.html> [Accessed 21 April 2017].
- IETF. 2006. The Secure Shell (SSH) Protocol Architecture. Available at: <https://www.ietf.org/rfc/rfc4251.txt> [Accessed 25 April 2017].
- Kasanen, L. 2013. Into the Core - A Look at Tiny Core Linux. Available at: <http://tinycorelinux.net/corebook.pdf> [Accessed 5 October 2016].
- Microsoft. N.d. Radius Protocol and Components. Available at: [https://technet.microsoft.com/en-us/library/cc726017\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc726017(v=ws.10).aspx) [Accessed 17 January 2017].
- NTP. N.d.a. Encryption. Available at: <http://www.ntp.org/ntpfaq/NTP-s-algo-crypt.htm> [Accessed 7 April 2017].
- NTP. N.d.b. What is NTP? Available at: <http://www.ntp.org/ntpfaq/NTP-s-def.htm> [Accessed 22 November 2016].
- Odom, W. 2008. CCNA ICND2 Official Exam Certification Guide, Second Edition. Indianapolis: Cisco Press.
- Omniseu. N.d. What is Etherchannel in Cisco Switches and Routers, What is Link Aggregation and what are PAgP LACP. Available at: <http://www.omniseu.com/cisco-certified-network-associate-ccna/what-is-etherchannel-in-cisco-switches-and-routers.php> [Accessed 15 November 2016].
- Peltonen, A. 2016. Application Delivery Controller Implementation to Cyberlab Data Center. Bachelor's Thesis. Kymenlaakso University of Applied Sciences.



Available at:

[http://theseus.fi/bitstream/handle/10024/110229/antti\\_peltonen.pdf?sequence=1](http://theseus.fi/bitstream/handle/10024/110229/antti_peltonen.pdf?sequence=1)  
[Accessed 25 October 2016].

Rouhiainen, K & Kettunen, M. 2015. Kyberturvallisuutta kehitetään joukolla. Koskinen 5/2015. Available at: <http://www2.kyamk.fi/Koskinen/052015/kyber.html>  
[Accessed 25 October 2016].

Techtarget. 2010. Virtualization hypervisor comparison. Available at:  
<http://searchservervirtualization.techtarget.com/tip/Virtualization-hypervisor-comparison-Type-1-vs-Type-2-hypervisors> [Accessed 1 November 2016].

Tiny Core Team. 2007. Introduction to Core. Available at: <http://tinycorelinux.net/intro.html> [Accessed: 13 December 2016].

VMware. N.d. Virtualization. Available at:  
<http://www.vmware.com/solutions/virtualization.html> [Accessed: 20 April 2017].

## Admin-context configuration

CG-FW1/pri/act/admin# show startup-config

```

hostname CG-FW1
domain-name ictlab.kyamk.fi
enable password 7illEt4F.u/O305N encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names

interface Management0/0
management-only
nameif management
security-level 0
ip address 172.18.2.23 255.255.255.0 standby 172.18.2.24

dns server-group DefaultDNS
 domain-name ictlab.kyamk.fi
pager lines 24
logging enable
logging timestamp
no logging hide username
logging standby
logging monitor informational
logging trap informational
logging asdm informational
logging facility 17
logging host management 172.18.2.40

mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route management 0.0.0.0 0.0.0.0 172.18.2.1 1

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00

aaa-server RADIUS protocol radius
aaa-server RADIUS (management) host 193.167.x.x
key *****
aaa-server RADIUS (management) host 193.167.x.x
key *****
user-identity default-domain LOCAL
aaa authentication ssh console RADIUS
aaa authentication http console RADIUS
aaa authentication enable console LOCAL
aaa authorization command LOCAL
aaa authorization exec authentication-server auto-enable
http server enable
http 10.69.0.0 255.255.0.0 management
snmp-server host management 10.69.2.16 poll community *****

no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
telnet timeout 5
ssh stricthostkeycheck
ssh 10.69.0.0 255.255.0.0 management
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1

```

```
no threat-detection statistics tcp-intercept
username admin password Z3Fv03WhCsh.PGtN encrypted
class-map inspection_default
match default-inspection-traffic
```

```
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
```

```
policy-map global_policy
class inspection_default
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect dns preset_dns_map
policy-map type inspect dns migrated_dns_map_1
parameters
  message-length maximum client auto
  message-length maximum 512
```

```
service-policy global_policy global
Cryptochecksum:fd759e86670e87b5e60c2881ecb8cc6b
: end
```

## System-context configuration

```
CG-FW1/pri/act# show startup-config
```

```
hostname CG-FW1
domain-name ictlab.kyamk.fi
enable password 7iIlEt4F.u/O305N encrypted
mac-address auto prefix 43990

interface GigabitEthernet0/0
description DC-SX_Te1/0/11
channel-group 1 mode active

interface GigabitEthernet0/1
description DC-SX_Te1/0/12
channel-group 1 mode active

interface GigabitEthernet0/2
shutdown

interface GigabitEthernet0/3
shutdown

interface GigabitEthernet0/4
description LAN Failover Interface

interface GigabitEthernet0/5
description STATE Failover Interface

interface Management0/0

interface Port-channel1
description DC-SX_Po2
lACP max-bundle 8

interface Port-channel1.2160
description NEST
vlan 2160 secondary 2260

interface Port-channel1.2180
description Frontend
vlan 2180 secondary 2280

interface Port-channel1.2181
description Backend
vlan 2181 secondary 2281

interface Port-channel1.2182
description Management
vlan 2182 secondary 2282

class default
limit-resource All 0
limit-resource Mac-addresses 16384
limit-resource ASDM 5
limit-resource SSH 5
limit-resource Telnet 5

ftp mode passive
pager lines 24
failover
failover lan unit primary
failover lan interface folinek GigabitEthernet0/4
failover replication http
failover link statelink GigabitEthernet0/5
failover interface ip folinek 172.18.4.1 255.255.255.0 standby 172.18.4.2
failover interface ip statelink 172.18.5.1 255.255.255.0 standby 172.18.5.2
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
ssh stricthostkeycheck
console timeout 0
```

```
admin-context admin
context admin
  allocate-interface Management0/0
  config-url disk0:/admin.cfg

context Level2
  allocate-interface Port-channel1.2181-Port-channel1.2182 vlan2181-vlan2182
  config-url disk0:/Level2.cfg

context Level1
  allocate-interface Port-channel1.2160 vlan2160
  allocate-interface Port-channel1.2180-Port-channel1.2181 vlan2180-vlan2181
  config-url disk0:/Level1.cfg

ntp authenticate
ntp server 193.166.5.197 source management prefer
ntp server 193.166.5.207 source management
ntp server 193.166.5.177 source management
ntp server 193.166.5.217 source management
username admin password Z3Fv03WhCsh.PGtN encrypted
prompt hostname priority state context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:738dd6667fd53fa010f090b1f3a0d5a6
: end
```

## Level1-context configuration

```
CG-FW1/pri/act/Level1# sh startup-config
```

```
hostname Level1
enable password 8Ry2Yjlyt7RRXU24 encrypted
names
```

```
interface vlan2160
 nameif NEST
 security-level 0
 ip address 172.16.0.5 255.255.0.0 standby 172.16.0.6
```

```
interface vlan2180
 nameif Frontend
 security-level 0
 ip address 172.18.0.5 255.255.255.0 standby 172.18.0.6
```

```
interface vlan2181
 nameif Backend
 security-level 100
 ip address 172.18.1.5 255.255.255.0 standby 172.18.1.6
```

```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list NEST-> extended permit ip 172.16.0.0 255.255.0.0 172.18.1.0 255.255.255.0
access-list NEST-> extended permit ip 172.16.0.0 255.255.0.0 172.18.0.0 255.255.255.0
access-list FE-> extended permit ip 172.18.0.0 255.255.255.0 172.18.1.0 255.255.255.0
access-list FE-> extended permit ip 172.18.0.0 255.255.255.0 172.16.0.0 255.255.0.0
pager lines 24
logging enable
logging timestamp
no logging hide username
logging asdm informational
logging facility 17
mtu NEST 1500
mtu Frontend 1500
mtu Backend 1500
monitor-interface NEST
monitor-interface Frontend
monitor-interface Backend
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group NEST-> in interface NEST
access-group FE-> in interface Frontend
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
no threat-detection statistics tcp-intercept
```

```
class-map inspection_default
match default-inspection-traffic

policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error

service-policy global_policy global
Cryptochecksum:f15d2d6881913d91aae88bd416faf1a4
: end
```

## Level2-context configuration

```
CG-FW1/pri/act/Level2# show startup-config
```

```
hostname Level2
enable password 8Ry2Yjlyt7RRXU24 encrypted
names

interface vlan2181
 nameif Backend
 security-level 0
 ip address 172.18.1.1 255.255.255.0 standby 172.18.1.2

interface vlan2182
 nameif MGMT
 security-level 100
 ip address 172.18.2.5 255.255.255.0 standby 172.18.2.6

same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list BE-> extended permit ip 172.18.1.0 255.255.255.0 172.18.2.0 255.255.255.0
access-list BE-> extended permit ip 172.18.1.0 255.255.255.0 172.18.1.0 255.255.255.0
pager lines 24
logging enable
logging timestamp
no logging hide username
logging asdm informational
logging facility 17
mtu Backend 1500
mtu MGMT 1500
monitor-interface Backend
monitor-interface MGMT
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group BE-> in interface Backend
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
no threat-detection statistics tcp-intercept
```



```
class-map inspection_default
match default-inspection-traffic

policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error

service-policy global_policy global
Cryptochecksum:fe8c39268c9cd51de5419cacfc14d6a5
: end
```