**Project WiFi 2.0**



# Table of Contents

[1 Table of Contents 2](#_Toc25581587)

[2 Document Version 2](#_Toc25581588)

[3 Introduction 3](#_Toc25581589)

[4 Equipment overview 3](#_Toc25581590)

[4.1 WLC 3](#_Toc25581591)

[4.2 Cisco Prime 3](#_Toc25581592)

[4.3 Cisco ISE 4](#_Toc25581593)

[5 Device Info 5](#_Toc25581594)

[6 WLC and Prime 8](#_Toc25581595)

[6.1 WLCs and AP failover 8](#_Toc25581596)

[6.2 SSIDs 8](#_Toc25581597)

[6.3 Per site configuration 9](#_Toc25581598)

[6.4 Cisco Prime 9](#_Toc25581599)

[7 ISE Radius (Internal) 9](#_Toc25581600)

[7.1 ISE Nodes 9](#_Toc25581601)

[7.1.1 Management 9](#_Toc25581602)

[7.1.2 PSN 9](#_Toc25581603)

[7.1.3 Topology 10](#_Toc25581604)

[7.1.4 Radius Flow 10](#_Toc25581605)

[8 ISE Guest 11](#_Toc25581606)

[8.1 ISE Nodes 11](#_Toc25581607)

[8.2 Topology 11](#_Toc25581608)

[8.3 Guest Flow 12](#_Toc25581609)

[8.4 Guest account creation 13](#_Toc25581610)

[8.4.1 Sponsor portal 13](#_Toc25581611)

[8.4.2 self-reg 13](#_Toc25581612)

# Document Version

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Revision Date | Author | Revision Summary |
| 0.1 | 2019-11-08 | Jonas Kalldert | First Draft |
| 0.2 | 2020-04-08 | Jonas Kalldert | Software Updates |
|  |  |  |  |

# Introduction

Mölnlycke Health Care is building a new global wifi infrastructure and authentication solution

To accommodate the ever-growing need of a stable and mission critical wifi Atea is designing, building and assisting in implementing this new solution.

The solution is designed around three HA WLC pairs, one in each continent where APs can failover to another continent WLC if needed. Management of the WLCs are handled with Cisco Prime Infrastructure. The Radius solution is designed with Cisco ISE where each continent has two PSN load-balanced behind a F5, management for these PSNs are in Amsterdam DC.

# Equipment overview

## WLC

The Cisco 5520 Wireless Controller provides centralized control, management, and troubleshooting for high-scale deployments in service provider and large campus deployments. It offers flexibility to support multiple deployment modes in the same controller: for example, centralized mode for campus, Cisco FlexConnect™ mode for lean branches managed over the WAN, and mesh (bridge) mode for deployments where full Ethernet cabling is unavailable. As a component of the Cisco Unified [Wireless Network](https://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/), this controller provides real-time communications between [Cisco Aironet® access points](https://www.cisco.com/en/US/products/ps5678/Products_Sub_Category_Home.html) and [Cisco Catalyst® access points](https://www.cisco.com/c/en/us/products/wireless/catalyst-9100ax-access-points/index.html), the [Cisco Prime® Infrastructure](https://www.cisco.com/en/US/products/ps11686/index.html), and the [Cisco Mobility Services Engine](https://www.cisco.com/en/US/products/ps9742/index.html), and is interoperable with other Cisco controllers.

For More Information:

<https://www.cisco.com/c/en/us/products/collateral/wireless/5520-wireless-controller/datasheet-c78-734257.html>

## Cisco Prime

Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from a single graphical interface. Cisco Prime Infrastructure provides network administrators a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

To overcome these challenges, IT professionals need a comprehensive solution to manage, visualize, and monitor the network from a single graphical interface. Cisco Prime™ Infrastructure provides lifecycle management, assurance visibility, and troubleshooting capabilities network-wide - from the wireless user in the branch office, across the WAN, and to the data centre. In essence, it is One Management and One Assurance, for One Network

For More Information:

<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/datasheet-c78-735696.html>

## Cisco ISE

Cisco ISE allows you to provide highly secure network access to users and devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.

For More Information:

<https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html>

# Device Info

MHC provides tree physical locations for the WLCs and allocates VMs in DC as follow:

All passwords are in a Keepass file that was handover at the same time as this document.

EMEA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | Device Type | Device name | DNS | IPs | Software | Note |
| CZ, Havirov | WLC | cz-hav-wlc01 | cz-hav-wlc01  .mhc.molnlycke.net | 10.244.33.130 | 8.5.151.0 | Management IP for HA |
|  |  |  | NA | 10.244.33.131 | NA | Redundancy Management cz-hav-wlc01-1 |
|  |  |  | NA | 10.244.33.133 | NA | Redundancy Management cz-hav-wlc01-2 |
|  |  |  | NA | 10.244.33.9 | NA | Service port cz-hav-wlc01-1 |
|  |  |  | NA | 10.244.33.10 | NA | Service port cz-hav-wlc01-2 |
|  |  |  | NA | 10.244.33.7 | 4.0(2h) | CIMC cz-hav-wlc01-1 |
|  |  |  | NA | 10.244.33.8 | 4.0(2h) | CIMC cz-hav-wlc01-2 |
| Amsterdam DC | VM | nl-int-ise01 | nl-int-ise01  .mhc.molnlycke.net | 10.244.2.156 | 2.4 patch 11 | Pri PAN |
|  | VM | nl-int-ise02 | nl-int-ise02  .mhc.molnlycke.net | 10.244.2.157 | 2.4 patch 11 | Sec PAN |
|  | VM | nl-int-ise03 | nl-int-ise03  .mhc.molnlycke.net | 10.244.2.158 | 2.4 patch 11 | Pri MnT |
|  | VM | nl-int-ise04 | nl-int-ise04  .mhc.molnlycke.net | 10.244.2.159 | 2.4 patch 11 | Sec MnT |
|  | F5 | Radius VIP | NA | 10.244.2.163 | NA | VIP for internal radius requests |
|  | VM | nl-int-isepsn01 | nl-int-isepsn01  .mhc.molnlycke.net | 10.244.20.16 | 2.4 patch 11 | ISE PSN |
|  | VM | nl-int-isepsn01 | nl-int-isepsn02  .mhc.molnlycke.net | 10.244.20.17 | 2.4 patch 11 | ISE PSN |
|  | VM | nl-int-cpi04 | nl-int-cpi04  .mhc.molnlycke.net | 10.244.2.162 | 3.7 Update 03 Device pack 2 | Cisco Prime |
|  | VM | nl-int-isegst01 | nl-int-isegst01  .mhc.molnlycke.net | 10.244.20.11 | 2.7 patch 0 | Gi0 Internal |
|  | VM | nl-int-isegst01 | NA / guestnode01  .molnlycke.com | 10.244.12.163 / 89.202.241.163 | 2.7 patch 0 | Gi1 External, DMZ IP NATed to public IP |
|  | VM | nl-int-isegst02 | nl-int-isegst02  .mhc.molnlycke.net | 10.244.20.12 | 2.7 patch 0 | Gi0 Internal |
|  | VM | nl-int-isegst02 | NA / guestnode01  .molnlycke.com | 10.244.12.164 / 89.202.241.164 | 2.7 patch 0 | Gi1 External, DMZ IP NATed to public IP |
|  | F5 | Guest VIP | guestsponsor  .mhc.molnlycke.net | 10.244.2.161 | NA | VIP for radius requests on guest network and portal for guest account creation |

AMER

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | Device Type | Device name | DNS | IPs | Software | Note |
| US, New York | WLC | us-nyc-wlc01 | us-nyc-wlc01  .mhc.molnlycke.net | 10.242.1.2 | 8.5.151.0 | Management IP for HA |
|  |  |  | NA | 10.242.1.4 | NA | Redundancy Management us-nyc-wlc01-1 |
|  |  |  | NA | 10.242.1.5 | NA | Redundancy Management us-nyc-wlc01-2 |
|  |  |  | NA | 10.242.1.20 | NA | Service port us-nyc-wlc01-1 |
|  |  |  | NA | 10.242.1.22 | NA | Service port us-nyc-wlc01-2 |
|  |  |  | NA | 10.242.1.21 | 4.0(2h) | CIMC us-nyc-wlc01-1 |
|  |  |  | NA | 10.242.1.23 | 4.0(2h) | CIMC us-nyc-wlc01-2 |
|  | F5 | Radius VIP | NA | 10.242.2.163 | NA | VIP for internal radius requests |
|  | VM | us-nyc-isepsn01 | us-nyc-isepsn01  .mhc.molnlycke.net | 10.242.20.16 | 2.4 patch 11 | ISE PSN |
|  | VM | us-nyc-isepsn01 | us-nyc-isepsn02  .mhc.molnlycke.net | 10.242.20.17 | 2.4 patch 11 | ISE PSN |

APAC

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | Device Type | Device name | DNS | IPs | Software | Note |
| MY, Kullim | WLC | my-kul-wlc02 | my-kul-wlc02  .mhc.molnlycke.net | 10.246.58.132 | 8.5.151.0 | Management IP for HA |
|  |  |  | NA | 10.246.58.134 | NA | Redundancy Management my-kul-wlc02-1 |
|  |  |  | NA | 10.246.58.135 | NA | Redundancy Management my-kul-wlc02-2 |
|  |  |  | NA | 10.245.105.157 | NA | Service port my-kul-wlc02-1 |
|  |  |  | NA | 10.245.105.159 | NA | Service port my-kul-wlc02-2 |
|  |  |  | NA | 10.245.105.158 | 4.0(2h) | CIMC my-kul-wlc02-1 |
|  |  |  | NA | 10.245.105.160 | 4.0(2h) | CIMC my-kul-wlc02-2 |
| CN, Hongkong | F5 | Radius VIP | NA | 10.247.2.163 | NA | VIP for internal radius requests |
|  | VM | cn-hkg-isepsn01 | cn-hkg -isepsn01  .mhc.molnlycke.net | 10.247.20.16 | 2.4 patch 11 | ISE PSN |
|  | VM | cn-hkg -isepsn01 | cn-hkg -isepsn02  .mhc.molnlycke.net | 10.247.20.17 | 2.4 patch 11 | ISE PSN |

# WLC and Prime

## WLCs and AP failover

All WLCs are configured to match each other to be able handle any AP. The priority configured on the APs are as follows:

EMEA APs:

1st cz-hav-wlc01

2nd us-nyc-wlc01

3rd my-kul-wlc02

AMER APs:

1st us-nyc-wlc01

2nd cz-hav-wlc01

3rd my-kul-wlc02

APAC APs:

1st my-kul-wlc02

2nd us-nyc-wlc01

3rd cz-hav-wlc01

## SSIDs

All Production SSIDs are configured with flexconnect.

The Guest SSID are configure either as flexconnect or Central depending on if the site has a local breakout or not.

When configuring a new SSID the ID should be ID 17 or above. All IDs should match between the WLCs.

The current ID design looks as follows:

|  |  |  |
| --- | --- | --- |
| ID | Profile Name | WLAN SSID |
| 17 | MHC\_GlobalSSID | mhc!global! |
| 18 | MHC\_Guest\_Local | MHCGUEST |
| 19 | MHC\_Guest\_Central | MHCGUEST |
| 20 | Reserverd | Reserverd |
| 21 | MHC\_warehouse | mhc!warehouse! |
| 22 | CZ-HAV-SSI | SSI |
| 23 | MHC\_warehouse\_GB-OLD | mhc!warehouse! |
| 24 | MHC\_warehouse\_SE-GOT | mhc!warehouse |
| 25 |  |  |
| 26 |  |  |
| 27 |  |  |
| 28 |  |  |
| 29 |  |  |
| 30 |  |  |

## Per site configuration

A Site needs the following configuration

An AP-Group to specify AP, SSID and RF Profile.

There are two configured RF-Profiles, one for 5ghz “molnlycke-default-a” and one for 2.4 “molnlycke-default-bg” that can be used as default. If there are specific RF needs on a specific site a new RF-Profile needs to be configured and put on that AP group.

A Flexconnect group to specify what vlan each SSID needs to be droped down to and to have working roaming within the site.

All this configuration must be the same on all WLCs to have a working WiFi in the case of AP failover to another WLC. Best way to do this is to use configuration templates in Cisco Prime.

## Cisco Prime

To have configuration to match between the WLCs configuration templates should be used.

Each site should also have a map uploaded to prime and APs correctly placed.

# ISE Radius (Internal)

## ISE Nodes

### Management

The management servers for the ISE deployment are located in AMS DC on VMs nl-int-ise01, nl-int-ise02, nl-int-ise03, nl.int-ise04.

These VMs where requested as Medium VMs with 16 CPUs, 64GB RAM and 1200 Gig Disk. Due to limitations from GTT only 12 CPUs was allowed per VM.

To allow for wired .1x on top of wireless two additional VMs should be deployed to split PAN and MnT nodes.

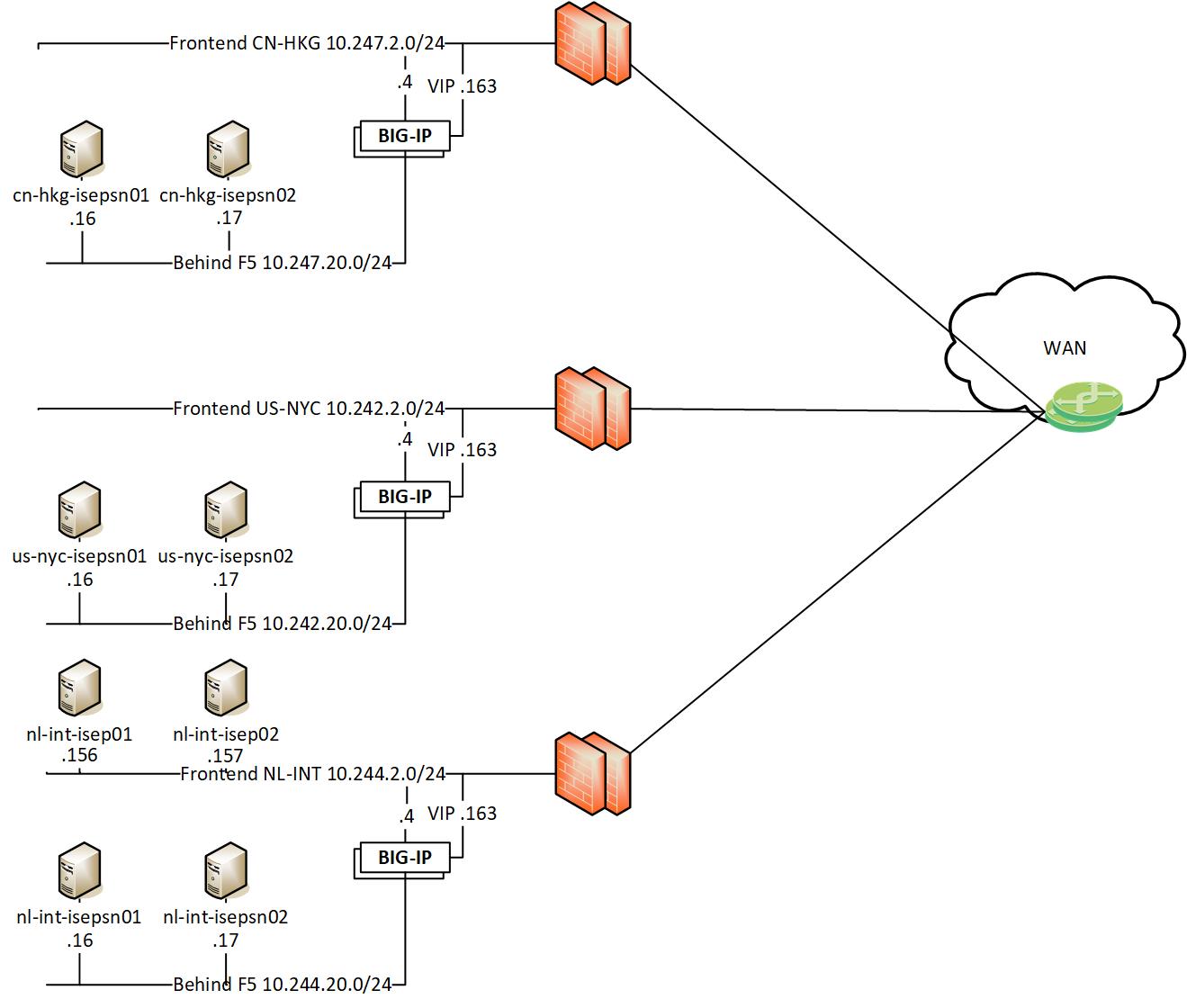
### PSN

All PSN VMs are configured as Small nodes with 12 CPUs, 16GB RAM and 200 Gig Disk.

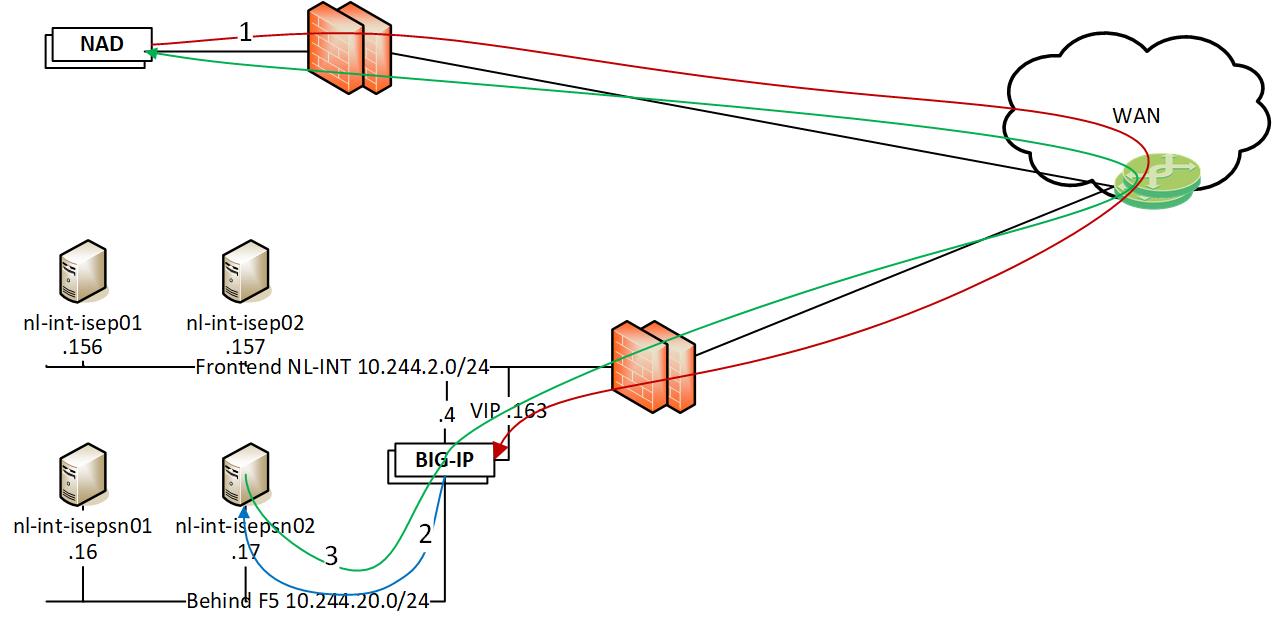
Each continent have two PSNs load balanced behind a F5. If more PSNs are needed du to higher Radius load more PSN VMs can be added in this design. This design also makes it easier to do maintenance on a VM if needed. In that case, disable the node in the F5 load balancing so no Radius packets are sent to that node. When the PSN is fixed, enable that node in the load balancing again.

The F5 are configured according to this guide: <https://community.cisco.com/t5/security-documents/how-to-cisco-amp-f5-deployment-guide-ise-load-balancing-using/ta-p/3631159>

### Topology



### Radius Flow



1. Radius request for new client from NAD (WLC/Switch) to VIP on F5
2. The request is load balanced between the nodes, in this case to nl-int-isepsn02
3. The PSN node responds to the NAD and are source NATed behind the VIP on the way back. (This is also the same flow for CoA. The PSN sends the CoA to the NAD and are source NATed behind the VIP)

# ISE Guest

## ISE Nodes

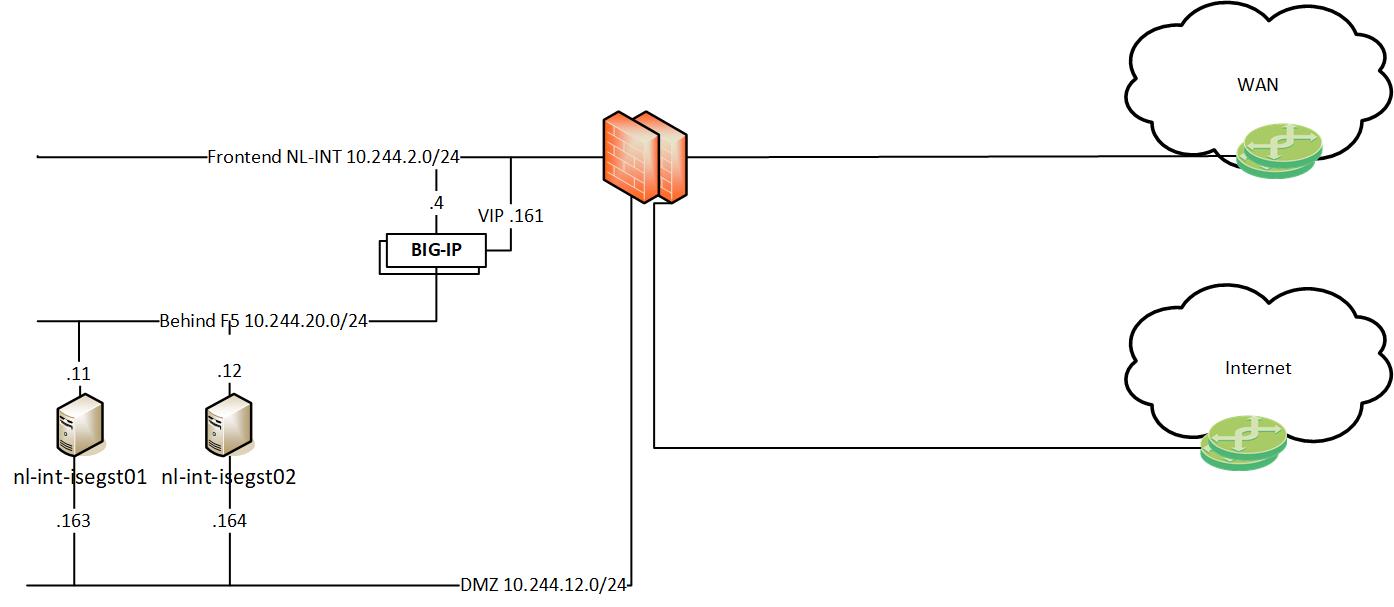
The ISE nodes for the guest solution are located in AMS DC on VMs nl-int-isegst01 (Pri PAN / Sec MnT / PSN) and nl-int-ise02 (Pri MnT / Sec PAN / PSN).

These VMs where requested as Medium VMs with 16 CPUs, 64GB RAM and 1200 Gig Disk. Due to limitations from GTT only 12 CPUs was allowed per VM.

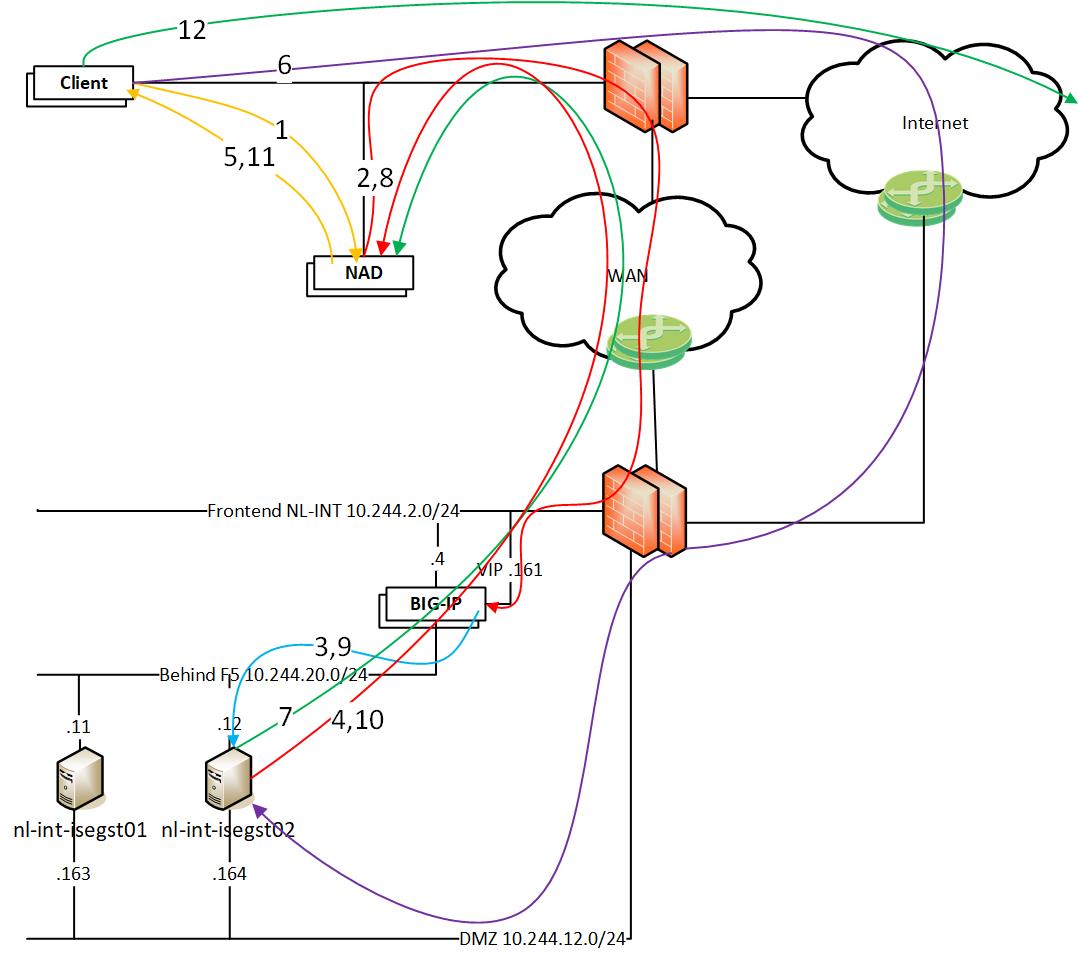
The nodes are configured with two interfaces Gi0 Internal and Gi1 External. Gi0 is load balanced behind the F5 to handle the radius requests from the WLC and also the guestsponsor portal is load balanced here.

The external interface is handling the guest splash page where the guest needs to provide credentials or requesting an account.

## Topology



## Guest Flow



1. Guest connects to the guest network
2. Radius request is sent from the NAD to the VIP
3. The request is load balanced between the nodes, in this case to nl-int-isegst02
4. The PSN answers the radius request with a web-redirect and an ACL to be applied to the client.
5. The client gets the web-redirect and is applied an ACL that only allows dns and communication with the public side of the PSN
6. The client is directed with the web-redirect to the public interface on the PSN on port 8445 and gets there over the internet.
7. When the client has authenticated via the guest web portal a CoA is sent to the NAD.
8. The NAD redoes the authentication for the client and sends a radius request to the VIP.
9. The F5 load balance the request and with the sticky configuration the same PSN will get the request.
10. The PSN knows the client and sends a correct access-accept with a guest ACL back to the NAD.
11. The client is allowed on the network and is applied a guest ACL that blocks internal networks.
12. The client can now surf the web.

## Guest account creation

### Sponsor portal

Guest accounts can be created by sponsors via guestsponsor.mhc.molnlycke.net

### self-reg

Guest can also request an account via the self-reg ling on the login page of the guest wifi. The guest fills in the required information and then the sponsor for the guest will receive an email to approve or deny the account