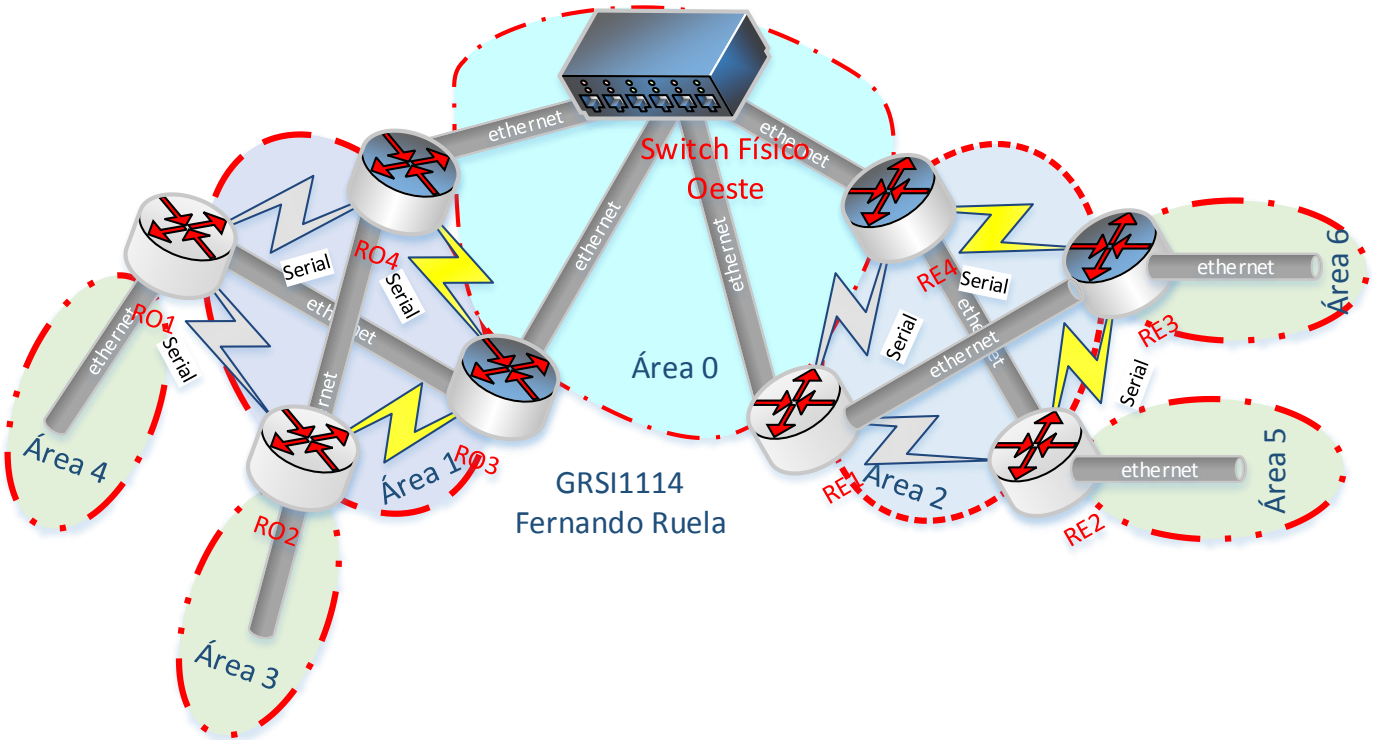
Projecto Final Sistemas Operativos GRSI1114



Índice do trabalho

Conteúdo

Layout lógico da estrutra de rede e servidores de um grupo

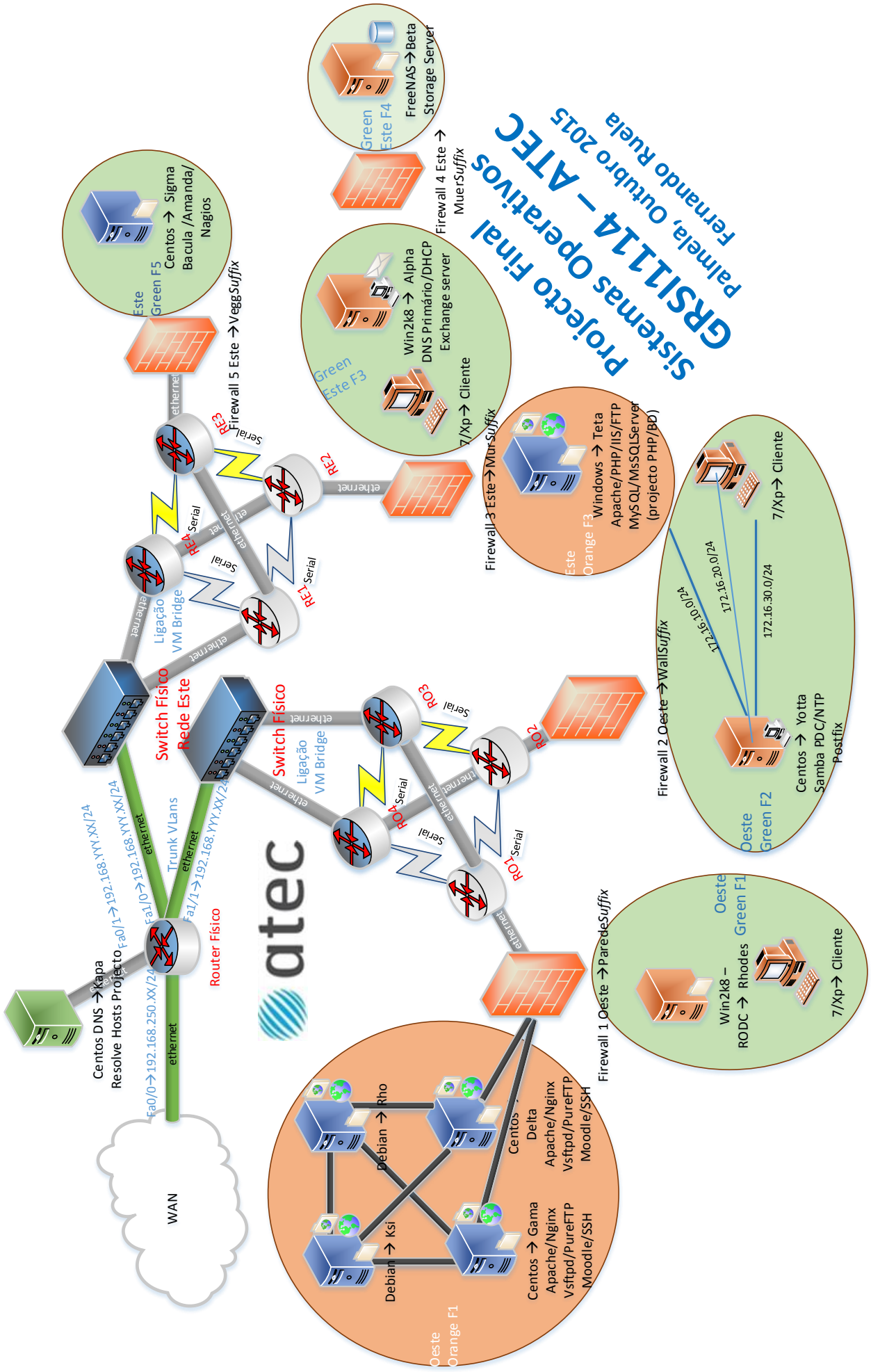


Figura 1

Layout lógico da estrutra de rede e servidores → Zona Oeste

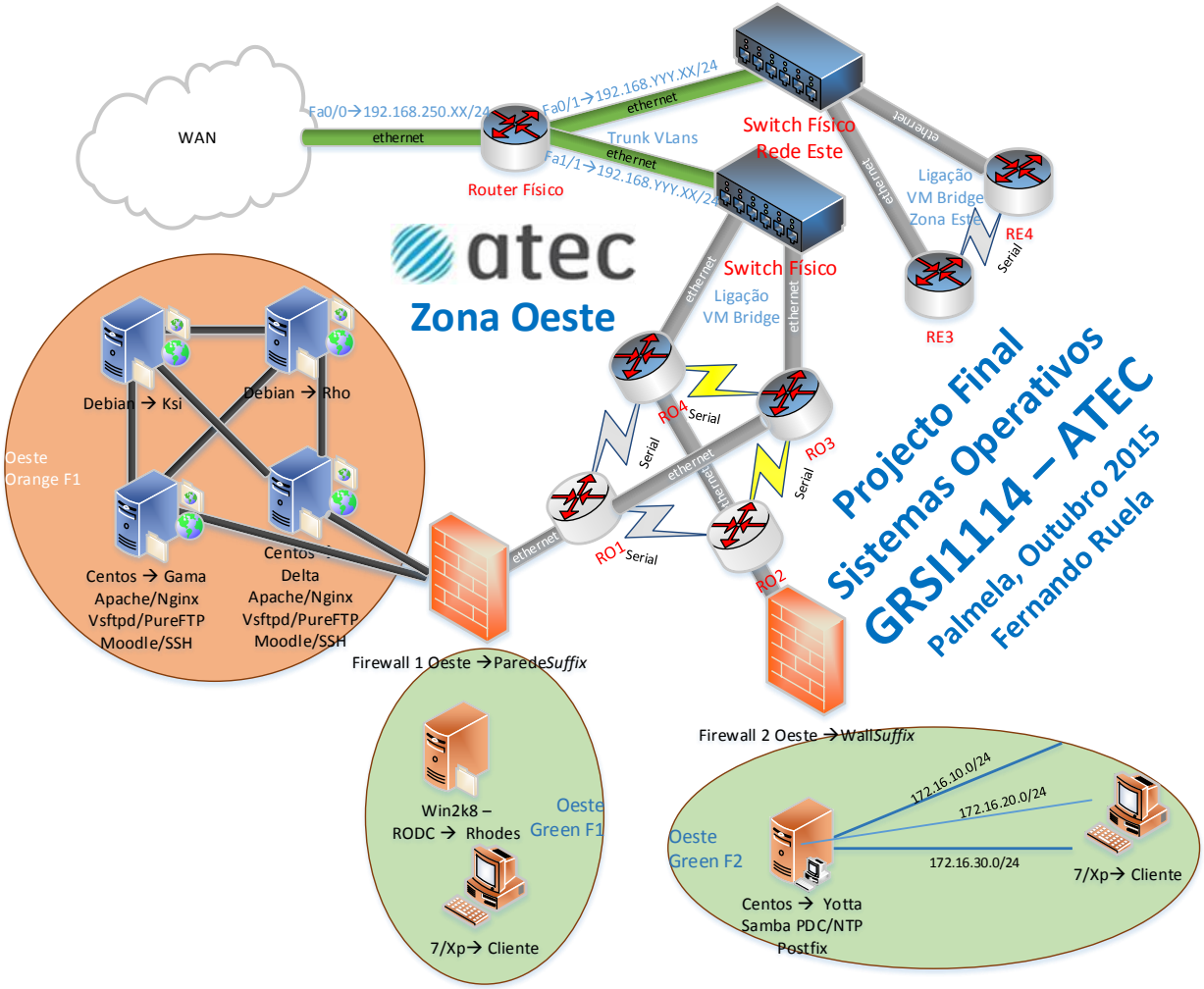


Figura 2

Layout lógico da estrutra de rede e servidores → Zona Oeste

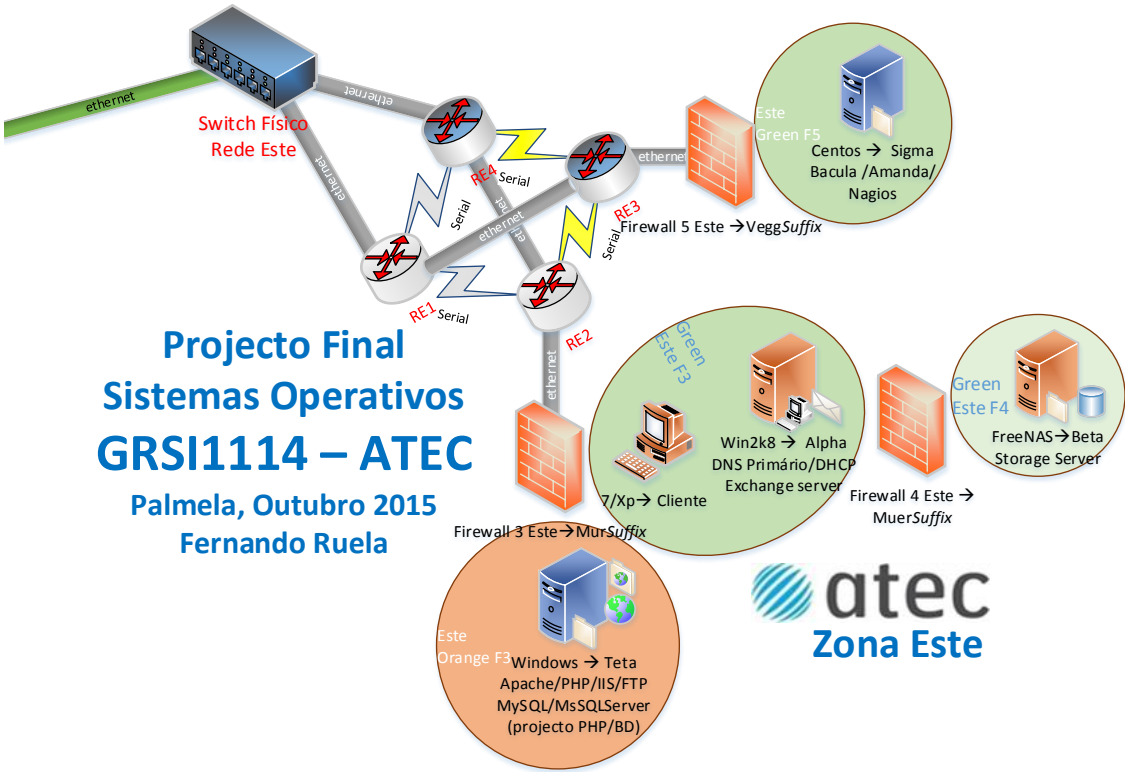


Figura 3

Tarefas a desenvolver no projecto Final Sistemas Operativos GRSI1114

Este trabalho consiste na configuração em máquinas virtuais (VMs) da estrutura de rede apresentada na Figura 1
Pretende-se implementar uma rede baseada em 10 servidores, 5 firewalls, 8 routers (virtuais) mais um router e 1 switch (estes últimos físicos).
Todas as especificações contidas no projecto terão que ser validadas em discussão final, onde será verificada a funcionalidade das mesmas.

Para cada solução apresentada (grupo de dois formandos) deve apresentar um relatório da instalação/configuração de todas as máquinas. Esse relatório deve respeitar as normas do documento standard e o seu conteúdo deve possibilitar a qualquer formando da turma, seguindo os diferentes passos de instalação, alcançar os resultados obtidos pelo grupo/individuo.
No relatório deve constar uma tabela com IPs/Redes e Macs utilizados. Aconselha-se a utilizar Macs definidos pelo formando, nomeadamente nas interfaces dos Firewall. Se necessário, deve-se considerar, os seguintes IPs para as interfaces RED dos Firewall e Xp Cliente (WAN) – 192.168.YY.X/24, sendo as letras YY e XX os numeros que pode consultar na tabela de IPs por grupo/formando.

No final, o relatório, deve apresentar uma conclusão sobre os aspectos técnicos das soluções encontradas. Valorizam-se sugestões que melhorem, a segurança, fiabilidade, usabilidade das soluções apresentadas.

O projecto final tem, para além da instalação e configuração dos sistemas, uma componente de metodologia de projecto. Essa metodologia diz respeito a uma planificação das etapas a devenvolver, uma vez que existem pontos críticos que são comuns a outros grupos. Isto é, para que determinadas tarefas sejam executadas existem configurações/instalações a desenvolver por terceiros (outro grupo) para que a completa execução de alguns pontos que são solicitados, sejam correctamente efectuados. Da mesma forma que um grupo depende de outro grupo, existirá outro grupo que depende de nós. Com este novo aspecto introduzido na execução do projecto, pretende-se abranger vertentes de responsabilidade para e de, outra equipa, o que sucede inúmeras vezes em empresas e inter-empresas.
Essa interacção com outros grupos deve ser acordada, entre as partes, e será igualmente avaliada

Peso da Avaliação

Projecto	Relatório	Funcionalidade	Conteúdo
Total	5 Valores	15 Valores	Fig1 → Todos os Grupos

Tabela 1

O relatório deve ser enviado, por email, dois dias antes da discussão/apresentação, para o meu email com CC para o email do coordenador do curso. Atraso na entrega do relatório, irá descontar 0,5 pontos/dia.

A discussão terá a duração de 1horas, sem preparação das VMs. Assim devem ensaiar as VMs no(s) PCs, antes da apresentação, visto que a duração apresentação/discussão do projecto será exclusiva para esse efeito!

O software utilizado será o apreendido durante as aulas, em termos de sistemas operativos:
- Servidores CentOS 6.6 /Debian 7/ Windows 2008/ Windows 7 / Windows XP . Pode incluir outras distribuições de Linux, desde que essa informação venha reflectida no relatório (configuração) e os formandos consigam defender a funcionalidade, durante a discussão do projecto
- Firewall → os firewall podem escolhidos da seguinte lista: Ipfire, PfSense, Smothwall, ClarkConnect, Zentyal, Endian Firewall, m0n0wall, Netdeep Cop, Shorewall, Untangle, PCX Firewall, WebCBQ Firewall, ZeroShell e IPCOP

Podem utilizar a mesma distribuição de firewall, nos firewall Oeste e Este..
- Máquinas de teste – Windows Xp/ Windows 7

Dimensione as máquinas virtuais de forma, a que, durante a verificação do projecto, possam ser executadas num PC da sala 0.21.

Diagrama Temporal de Execução (DTE)

Outro aspecto neste projecto, é a apresentação de um diagrama temporal, de instalação, configuração e testes de todas as acções solicitadas neste documento. Esse diagrama temporal, deve indicar dias (do calendário) /duração das acções e deve ser entregue até 2 dias após a data da recepção final do projecto
Esta calendarização das acções a desenvolver (Diagrama Temporal Execução – DTE) tem dois objetivos principais:

1) Levar os formandos a estabelecer e a organizar um calendário para a execução do projecto
2) Durante a execução das tarefas, permitir ao grupo avaliar "em que ponto" estão comparativamete ao previsto.

Este DTE não será para avaliação, apenas introduz a percepção do factor temporal na execução de um projecto, e assim fornecer aos formandos a perspectiva da evolução comparativa entre o previsto e o realizado.
No final, do projecto deve resultar um DTE exacto, com tempos correctos dispendidos nas tarefas., que também deve de ser entregue para ser discutido com o formador na tentativa de entender os desvios decorrentes da execução realtivamente ao previsto.
Com esta experiência, capacitam-se os formandos para uma prática corrente realizada em empresas, previsão de execuçao de um projecto e conclusão de tarefas em periodo determinado

Grupos Projecto Final Sistemas Operativos GRSI1114, Domínios e Redes

Num	Gama IPs ext WAN	Dominio Windows/Linux	Formando 1	Formando 2	Suffix
1	192.168.110. 0/24	André Vaz/Nuno Barroca	André Vaz	Nuno Barroca	AVNB
2	192.168.120. 0/24	Diogo Tavares / Paulo Soares	Diogo Tavares	Paulo Soares	DTPS
3	192.168.130. 0/24	Gabriel Azul / Tiago Silva	Gabriel Azul	Tiago Silva	GATS
4	192.168.140. 0/24	Diogo Cardoso /Guilherme Carvalhol	Diogo Cardoso	Guilherme Carvalho	DCGC
5	192.168.150. 0/24	David Sobral / Nuno Carvalho	David Sobral	Nuno Carvalho	DSNC
6	192.168.160. 0/24	João Dias / Rui Guerreiro	João Dias	Rui Guerreiro	JDRG
7	192.168.170. 0/24	Justino Crispim / Rafael Soaresl	Justino Crispim	Rafael Soares	JCRS
8	192.168.180.0/24	Fabio Rafael	Fabio Rafael		FR

Tabela 2

As VMs devem de ter o nome segundo este critério: hostname_Suffix_GRSI1114 → ALPHA_FR_GRSI1114

Hostname das Firewall → F1 = ParedeSuffix ; F2 = WallSuffix ;F3=MurSuffix; F4=MuerSuffix; F5=VeggSuffix

NOTA:
TODAS as passwords devem ser "Passw0rd", e os users, que não estão configurados por defeito "atec".
Os IPs e redes a utilizar são ao seu critério mas devem, obviamente, ser indicados no relatório de funcionamento. Sugere-se que tenha na sua posse, durante a discussão/apresentação tabelas de IPs/redes/macs e portos utilizados na configuração dos sistemas

Os utilizadores do sistema, que entretanto criar, devem de ter o nome de colegas da turma

Todos os testes de: acesso a páginas web, acesso a servidores de ftp, acesso a webmail (Exchange ou Postfix) devem de ser efectuados da wan. Considere o host com um ip da mesma rede do router físico. Não são aceites ligações Roadwarrior

Serviços em ALPHA

A) O servidor **ALPHA** deve funcionar como Primary Domain Controller do domínio *apelido.local*

A.1) Nele deve funcionar o DNS, em modo primário. Deve ser servidor primário para os PCs que se encontram na zona Green ESTE, do firewall MurSuffix.

A.2) No entanto se forem efectuados pedidos a este serviço, ele deve indicar IP||FQDN do host que se encontra na Zona Green Este. Independentemente da forma como está definido o IP do host (estático ou dinâmico)

A.3) O servidor teve ter o serviço de correio (Exchange 2010) e proporcionar email para todos os users do domínio. Estes, quando fazem logon num pc cliente, o seu Outlook deve estar configurado com as características que lhes permitam enviar/receber emails. Agendar reuniões, marcar tarefas, etc..

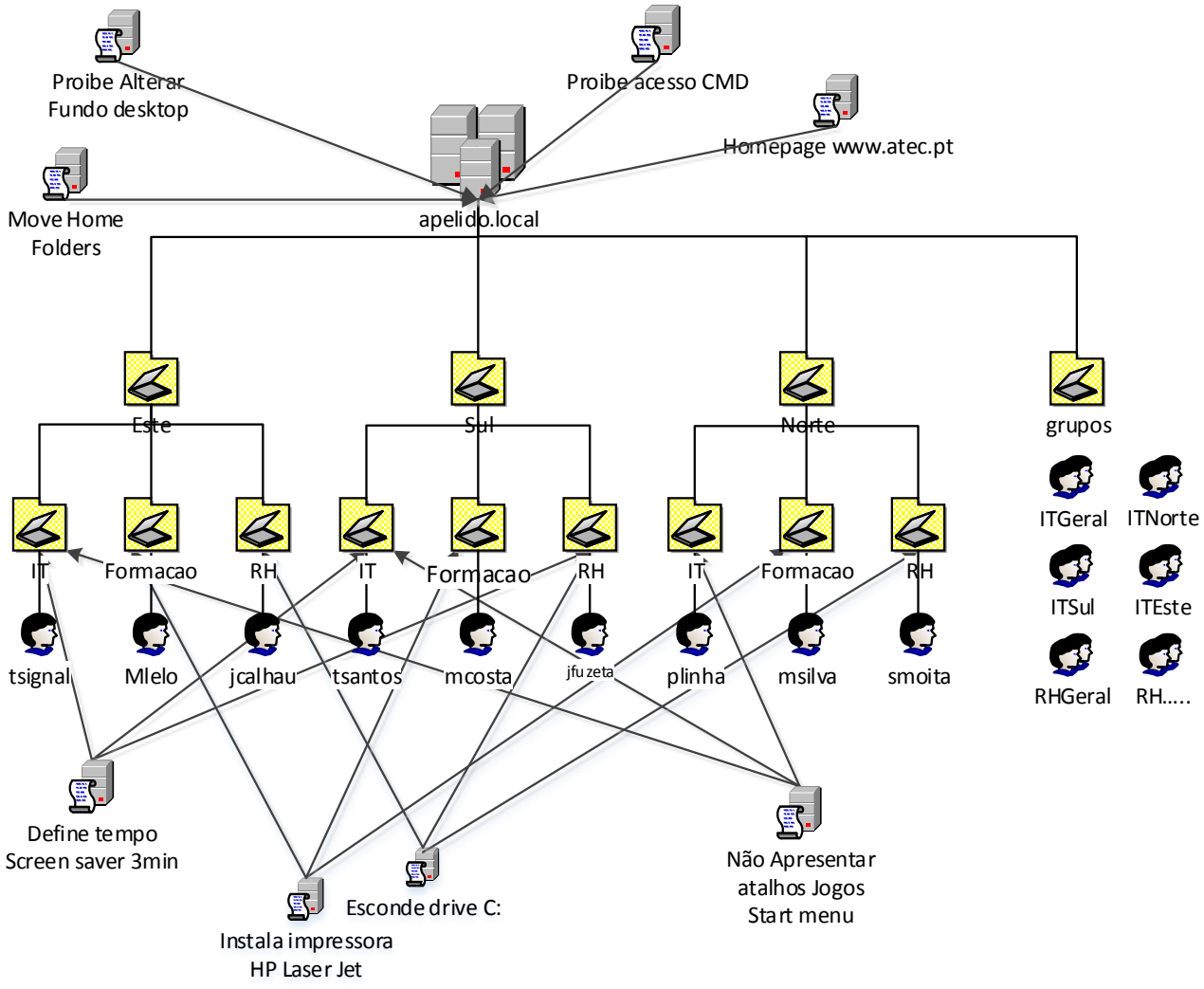
A.4) As "stores" do Exchange devem de estar alojadas no servidor FreeNAS (**BETA**)

A.5) Os users da OU ESTE não podem enviar email, fora do horário 9h-19h.

A.6) Todos os users devem poder aceder, via HTTPS ao seu correio, independentemente de se encontrarem na WAN (não se considera a utilização da VPN para este efeito.

A.7) Na AD, deve ser criada a seguinte estrutura de OUs, bem como as GPOs e restrições de acesso aos utilizadores do domínio.

A.8) Configure o DHCP, por forma a que forneça, informação relevante aos clientes: gateway, DNS primário e Secundário, nome do domínio, NTP1 e NTP2



A.9) O NTP primário deste servidor deve ser o NTP existente em **YOTTA**

A.10)Crie os utilizadores e grupos, identificados na próxima tabela

Nome	**Apelido**	**Login**	**OU||Grupo**	**Password**
Tiago	Signal	Tsignal	IT	Passw0rd
Miguel	Lelo	Mlelo	Formacao	Passw0rd
Jonas	Calhau	Jcalhau	RH	Passw0rd
Tomas	Santos	Tsantos	IT	Passw0rd
Marta	Costa	Mcosta	Formacao	Passw0rd
Joao	Fuzeta	Jfuzeta	RH	Passw0rd
Pedro	Linha	Plinha	IT	Passw0rd
Manuel	Silva	Msilva	Formacao	Passw0rd
Sandra	Moita	Smoita	RH	Passw0rd

A.11)Os perfis e homes folders (My documents, Downloads, My pictures, etc) dos utilizadores estão localizados no servidor **BETA**.

A.12)Nas Homes dos users, apenas aos próprios deve ser possivel aceder, alterar e executar

A.13)Cada grupo (IT, FORMACAO, RH) deve ter uma pasta para o respectivo grupo, situada no **BETA**, com permissões totais (Leitura/escrita/execução) para o respectivo grupo.

A.14)O grupo IT deve ter permissões de escrita na pasta do grupo RH e de leitura pasta FORMACAO

A.15) O grupo FORMACAO deve ter acesso de leitura às pastas dos grupos anteriores

A.16) O grupo RH tem permissões de escrita na pasta do grupo FORMACAO

A.17)Realize os procedimentos necessários. Quando um user faz login, na zona Este, é mapeada a drive **S:** correspondente à uma share, limitada a 100MB por user, para que possa colocar informação importante

A.18)Crie uma GPO para todos os utilizadores do domínio que não lhes permita acederem à linha de comando (CMD)

A.19) Como os administradores do domínio, assim como o pessoal IT necessitam de ter acesso à linha de comando, proceda para que estes possam aceder à linha de comando.

A.20)Crie uma GPO que coloque imagens (à sua escolha) de desktop específicas (uma por departamento – RH, IT, FORMACAO) quando um user, pertencente a esse departamento realizar logon num pc. Os users não podem alterar a imagem.

A.21) Todos os users do dominio têm a home page do IE **www.atec.pt** Não podem alterar esta página

A.22) Crie uma política no domínio nomegrupo.local que esconde a **drive c:** aos users das OUs RH

A.23)Crie outra GPO aplicada aos users do IT que defina o tempo **screen saver** de 3minutos

A.24) Aos users inseridos nas OUs IT não deve surgir o *atalho dos jogos* no menu iniciar

A.25)Aos users das OU Formação, deve ser instalada uma impressora, assim que realizam o login

A.26)Configure o servidor **ALPHA**.apelido.local, por forma que seja possível ao utilizador "atec" aceder remotamente a este servidor, a partir da estação de trabalho (windows XP/7 na Zona Green Norte do RODC do grupo com quem está a colaborar no projecto)

A.27)Crie uma GPO que instale, para os users das OUs IT, o software OpenVPN, na estação de trabalho em que estes efectuam o login

A.28)Backup do *Schema* e *Sysvol* da AD , todas as noites ás 02:00h para o servidor **SIGMA**

Serviços em YOTTA

C) O servidor **YOTTA** deve ter em funcionamento os serviços: DHCP, DNS, serviço de impressão CUPS, serviço de email Postfix para além de outros que entretanto considere necessários. Será também um PDC onde terá um comportamento semelhante a um servidor Windows com AD. Assim, com a configuração correcta do serviço SAMBA, de forma a que funcione como um PDC, deve ser possivel colocar no dominio → **Outroapelido.local** as máquinas windows (XP/7) que estejam na rede 172.16.20.0/24. A "adição" destas máquinas deve de respeitar o mesmo procedimento que é executado quando se coloca um cliente num domínio Windows (identificação do domnio → identificação de user/password com privilégios de adição de máquinas ao domínio). Não serão necessárias GPOs para este dominio.

C.1) O servidor **YOTTA** tem duas interfaces. Uma está ligada á zona Green do firewall **WallSuffix**, outra está configurada com três subinterfaces. Cada subinterface tem associado um FQDN e domínio. Assim:

Eth1:1→ Rede 172.16.10.0/24 FQDN → lua.zona.local;
Eth1:2→ Rede 172.16.20.0/24 FQDN → sol.outroapelido.local;
Eth1:3→ Rede 172.16.30.0/24 FQDN→ terra.dominio.local.

C.2) Qualquer que seja o trafego que originário do YOTTA, com destino á interface Green do firewall **WallSuffix,** deve ter correspondência NAT, no **YOTTA**.

C.3) O DHCP deve fornecer a informação para cada um dos hosts – referente á rede onde se encontram associados - consistindo em: Dominio; Gateway; DNS server; NTP server (**YOTTA**); tempo de leases (mínimo e máximo)

C.3.1) O DHCP deve colocar na rede 172.16.10.0/24, os hosts que contenham no hostname **???PC???**

- Pools e leases ao seu critério

C.3.2) Na rede 172.16.20.0/24 os hosts cujo o seus hostname tenham as seguintes caracteristicas **??WS??**

- Pools e leases ao seu critério

C.3.3) Na rede 172.16.30.0/24, quaisquer hosts que não se encontrem na situação dos pontos anteriores

- Pools e leases ao seu critério

C.3.4) Crie uma reserva de IP, com o nome "Impressora da Rede", para o host que se apresente com o MAC 08:00:27:11:23:45, com o IP 172.16.10.45

C.4) As shares do samba devem estar montadas sobre um raid 5, por software. O RAID5 assenta em 4 partições de 500MB, (discos de 1GB), sendo uma partição spare. E deve ser apresentado ao sistema no ponto de montagem /mnt/raid. Assim adicione 4 discos de 1GB, e particione cada disco a +- 500MB

C.5) Com as restantes partições de 500MB – dos discos anteriores, crie um sistema em LVM, montado em /mnt/LVM. Designação do LVM, grupos lógicos, etc, á sua escolha. Utilize este "disco" LVM para disponibilizar espaço, que considere necessário, para atribuir a grupos/users do projecto

C.6) Deve restringir o espaço disponível por utilizador, na share, para 100MB e deve de emitir uma mensagem quando atingir os 90MB

C.7) O servidor deve ter o Bind instalado para as três redes, e este deve de funcionar em Dynamic DNS, para todas as zonas. Qualquer pedido que lhe seja dirigido, e esse pedido não constar das suas zonas (directas e/ou dinâmicas) deve ser encaminhado para o servidor de DNS **Kapa**

C.8) O serviço CUPs deve facultar a impressora HP Laser jet 2100, aos clientes da rede (dominio **Outroapelido.local**).

C.9) Neste servidor deve estar instalado o serviço de email baseado em Postfix, e Dovecot. Onde cada utilizador do sistema terá uma conta de email tipo→ nomeuser@outroapelido.local .

C.10) Deve ser possível enviar emails para o exterior (Gmail, Hotmail, etc, por ex.)

C.11) Deve ser possível aceder da WAN, via WebMail ás contas de correio dos users com a interface disponibilizada pelo Squirrelmail, que está instalado e configurado no **YOTTA**, para visualização/envio de emails

C.12) O **YOTTA** deve sincronizar o serviço de tempo, tendo como stratum superior, situado na WAN, e será em simultâneo o NTP principal da sua rede. Qualquer servidor de NTP, deve de sincronizar o serviço de tempo com o **YOTTA**

C.13) O serviço de SSH, para além da autenticação ser efectuada com par de chaves privada/pública, e deve estar restringido ao horário das 9h às 12h e das 14h às 16h

C.14) Pode instalar uma aplicação de gestão de servidores como o Webmin ou ISPconfig **(não cotado)** para auxiliar a administração do servidor

C.15) O backup diferencial da informação referente às configurações do sistema, shares, home folders, etc, deve de ser efectuado todos os dias às 23h, para o servidor **SIGMA**.

Backup integral sábados 8:00

Servidor TETA

D) Este servidor irá conter os projectos de base de dados e PHP, desenvolvidos noutras disciplinas, os quais não serão cotados. O que sera sujeito a cotação é o acesso á essas base de dados ou websites, que devem de funcionar sobre SSL/TLS. Aproveitando a existência do serviço IIS – necessário ao funcionamento do projecto de base de dados – será solicitado a existênica de uma página Web, assim como o serviço de FTP.

D.1) Porto para o projecto de base de dados → 34567

D.2) Porto para o projecto de PHP → 45678

D.3) No **TETA** deve configurar uma página web, que deve funcionar em https, e com autenticação de utilizadores. Só podem aceder á página os users que pertencem á *Formação* . Esta autenticação deve ser validada na AD do **ALPHA** Conteúdo da página: " Site exclusivo de formandos" O porto para acederem é o 2239

D.4) Como o IIS também está agregado a serviços de FTP, deve configurar este serviço, onde só podem aceder os users da *Formação* . Estes users estarão em *jailroot* e só podem realizar o download de ficheiros.

Serviços em Kappa

E) O servidor **Kappa** tem o papel de DNS da "rede do projecto", o qual irá pesquisar na WAN, todos os registos de FQDNs. domínios, registos MX, etc. que não estejam registados nas suas zonas. Assim todos os DNS da rede (Zona Este e Oeste) devem de encaminhar os seus pedidos para este DNS. O **Kappa** terá de fornecer a resolução de nomes para IPs para toda a rede.

Serviços na DMZ Orange Este firewall Parede*Suffix*

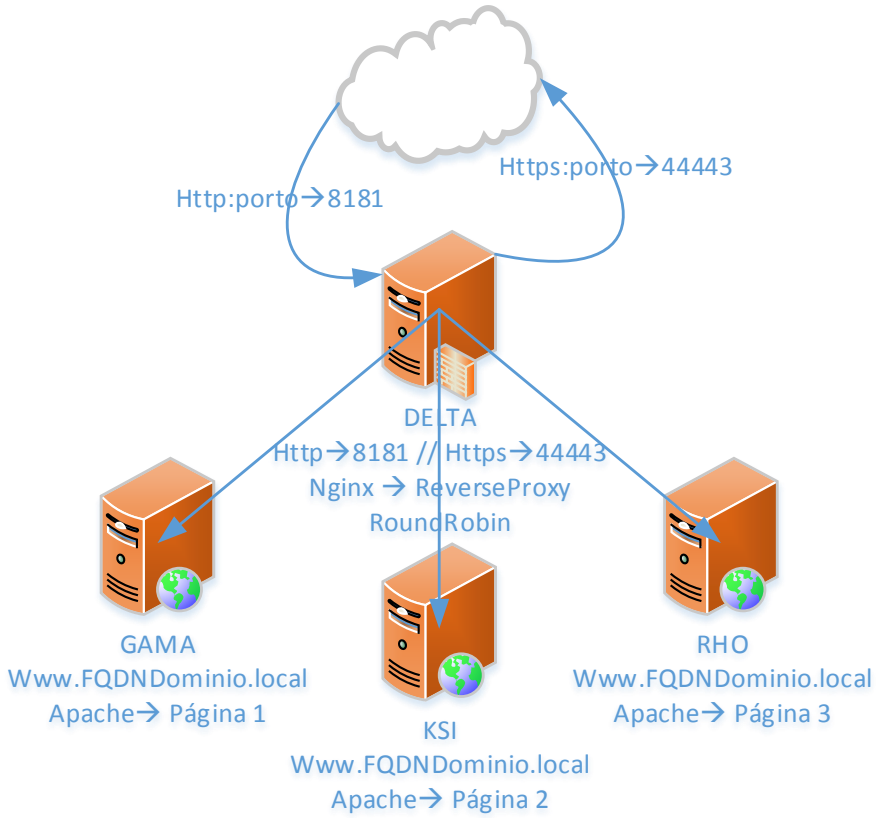
F) Nesta DMZ podemos encontrar os serviços web "abertos" para o exterior. A zona consiste em quatro servidores virtualizados (2 Centos & 2 Debian), interligados entre sí e configurados de forma a promover um sistema "Fault tolerance" e "High availability" aos serviços, Web, FTP e CMS. Assim os dados que são disponibilizados aos clientes, bem como os serviços, estarão sempre disponíveis, ainda que um dos quatro servidores, ou as suas ligações, tenham um quebra. O firewall **ParedeSuffix**, deve de estar a funcionar, para a DMZ Orange Este Firewall, em "Fault Tolerance" e/ou balanceamento de carga. O serviço http, será assegurado pelo Apache & Nginx; e o serviço FTP pelos serviços Vsftp e PureFTP, tanto para users virtuais, como para users "locais". Terá igualmente um serviço Web, a funcionar com "Reverse Proxy" e no modo "Round Robin". O CMS Moodle, terá igualmente as suas bases de dados assentes no sistema "Fault Tolerance". Os testes a efectuar devem ser realizados a partir da WAN e de um qualquer ponto/área proveniente dos projectos dos outros grupos

NOTA: Os portos e FQDNs dos sites (http/ftp), indicados na alíneas seguintes, dizem respeito a interface WAN do Firewall **ParedeSuffix**

F.1) Os servidores **DELTA** e **GAMA** serão praticamente "gémeos". Os serviços instalados e configuradados num servidor, serão igualmente, noutro com devidas alterações de IPs utilizados nas interfaces e serviços. Desta forma vamos apenas considerar a configuração do servidor **DELTA** , visto que o **GAMA** será "idêntico"em Linux terão o serviço HTTP baseado em duas aplicações: Apache e Nginx. Todos os sites estarão a funcionar sobre o **DELTA** por razões de economia de recursos dos PCs utilizados no projecto

F.1.1) Terá um sistema de redundância de sites http a funcionar em RoundRobin, com reverse proxy (Nginx). Onde o pedido chega no porto 8181 e a resposta é enviada em SSL/TLS porto 44443. Conteúdo dos sites (desenvolvidos sobre o Apache) Server1**(GAMA)** →" Site Reverse proxy –Site1 – *(Nome do servidor onde está o conteúdo da página armazenada)* " ; Server2 **(KSI)** →" Site Reverse proxy –Site2 - *(Nome do servidor onde está o conteúdo da página armazenada)*"; Server3 **(RHO)**→" Site Reverse proxy –Site3 *(Nome do servidor onde o*

conteúdo da página armazenada)". Quando o user pressiona em **F5** ou faz *refresh* ao browser, este apresenta, alternadamente o conteúdo de cada um dos sites. A resposta, enviada para o cliente estará encriptada em SSL/TLS. Ver figura seguinte



F.1.2) Como é pretendido redundância de resposta, deve realizar a "mesma" configuração no **GAMA**, para garantir que, se o servidor **DELTA** ficar inoperativo, os clientes vão continuar a aceder ás páginas que estão a funcionar em Round Robin. As tarefas a desenvolver nas seguintes alíenas devem de ser implementas quer no servidor **DELTA** quer no servidor **GAMA**

F.1.3) Site desenvolvido em Apache que opera no porto 3444, com autenticação na Active Directory do servidor **RHODES**. Permite apenas a "entrada" de users que pertençam ao grupo IT Conteúdo: " Site com autenticação na AD . Nomes dos membros do grupo".

F.1.4) Com o Nginx desenvolver um site que opere no porto 33333, que solicite a autenticação para do utilizador: atec / Passw0rd.

- Conteúdo da página: Título "GRSI1114"; "Página dos GRSI1114 Troinos – Já falta pouco! Quase a terminar"

F.1.5) Uma terceira página para acesso SSL/TLS, desenvolvida sobre o Apache, que aceita ligações no porto 44444

- . Conteúdo da página: "Curso de Gestão de Redes Informáticas, página segura com SSL/TLS". Título --> "Formandos de Redes – Serviços Web"

F.1.6) No porto 4343 deve estar a funcionar a plataforma de CMS Moodle. Sobre esta ligação encripatada com SSL/TLS, o Moodle, configurado de uma forma "básica" apenas com a possibilidade de um user (atec/passw0rd) poder aceder a um curso. As base de dados que o Moodle utiliza, devem estar alojadas nos servidores **RHO e KSI**

F.2) O FTP do projecto assenta em dois serviços: O VSFTP e o PureFtp. As configurações que realizar para um dos serviços de FTP, deve igualmente para o outro. A funcionar, obviamente em portos diferentes.

Nota: as pastas de upload e download *genéricas* do VSFTP e PureFTP devem residir em RHO e KSI

F.2.1) VSFTP → O serviço VSFTPD deve funcionar sobre dois daemons. Um será utilizado pelos users do sistema (users de DELTA – pode criar três ou mais users para o efeito (ex: user1; user2; user3) Um dos users está em "chroot" (user3). O user1, não consegue aceder por FTP. Este daemon de VSFTP deve escutar o porto 23232 (comandos) e transferir data no porto acima de 55000

F.2.2) Outro daemon para virtual users (porto de comandos e dados : os por defeito) O VSFTP (virtual users) deve permitir download de ficheiros por users anonymous, mas não o upload. O directório onde se encontram os ficheiros deve ser /home/ftp.

F.2.3) Crie uma lista de virtual users (Lilo, Lol, Lelo) onde cada um pode enviar e receber ficheiros, no entanto estarão em jailroot, nos directórios onde se logan (ex: /home/ftp/lilo)

F.2.4) O VSFTP, para os virtual users, deve estar a funcionar com SSL/TLS, isto é deve aceitar e inicializar o serviço por encriptação por SSL. Deve criar uma chave para o efeito

F.3) PureFtp→ O serviço PureFtp deve funcionar sobre dois daemons. Um será utilizado pelos users do sistema (users de **DELTA** – pode criar mais três ou mais users para o efeito (ex: user4; user5; user6).

F.3.1) Este daemon de FTP deve escutar o porto 51515 (comandos) e transferir data no porto acima de 52000 , outro daemon será utilizado com virtual users (porto de comandos 53332 e de dados acima de 56000). Um dos users está em "chroot" (user5). O user6, não consegue aceder por FTP

F.3.2) O PureFtp (virtual users) deve permitir download de ficheiros por users *anonymous*, mas não o upload. O directório onde se encontram os ficheiros deve ser /home/pureftp.

F.3.3) Crie uma lista de virtual users (Lili, lolo, lulu) onde cada um pode enviar e receber ficheiros, no entanto estarão em jailroot, nos directórios onde se logan (ex: /home/pureftp/lili)

F.3.4) O PureFTP, para os virtual users, deve estar a funcionar com SSL/TLS, isto é deve aceitar e inicializar o serviço por encriptação por SSL. Deve criar uma chave para o efeito

F.4) Backup das Bases dados do Moodle; pastas contendo o conteúdo dos sites, e locais de upload/download dos serviços de FTP; pastas com as configurações do serviços para o servidor **SIGMA**, todos os dias ás 08:00h

Serviços em Rhodes

G) O servidor **Rhodes** está a funcionar numa filial da empresa, na zona Este, como Read Only Domain Controller. Este servidor deve fornecer os serviços de DNS, DHCP aos clientes da Zona Green Este do firewall **ParedeSuffix**. O Primary Domain Controller deste RODC, é o servidor **Alpha do outro grupo.** Para que seja possivel configurar o servidor **Rhodes,** os dois grupos devem de trabalhar em conjunto – planear, instalar e testar, servidor **ALPHA,** VPN, roteamento nos routers físicos e virtuais. A **VPN** entre a Zona Este (**Rhodes**) e Zona Oeste Firewall MurSuffix (**Alpha outro grupo**) é da responsabilidade do grupo que detém o RODC. Esta VPN pode ser baseada em IPSEC ou OpenVPN

G.1) O DNS deve receber as zonas do servidor de DNS do **ALPHA**. Deve funcionar como "slave" do DNS do **ALPHA**.

G.2) O serviço de tempo deve ser actualizado no servidor NTP **ALPHA**.

G.3) O DHCP deve indicar as informações necessárias aos clientes para que estes possam utilizar os serviços existentes na rede.

G.4) O **RHODES** só deve ser permitir a autenticação de users que estejam na OU Norte

G.5) Teste com novos utilizadores, que entretanto coloca na OU Este, podem fazer a autenticação no **RHODES,** todos os outrso users que fiquem sob outras OUs da AD, não conseguem realizar o login no **RHODES**

G.6) Crie uma GPO, em ALPHA, para a OU Este, que force a utilização da home page, www.atec.pt, para o browser IExplorer, dos users daquela OU

G.7) Backup do *Schema* e *Sysvol* da AD , todas as noites ás 03:30h para o servidor **SIGMA**

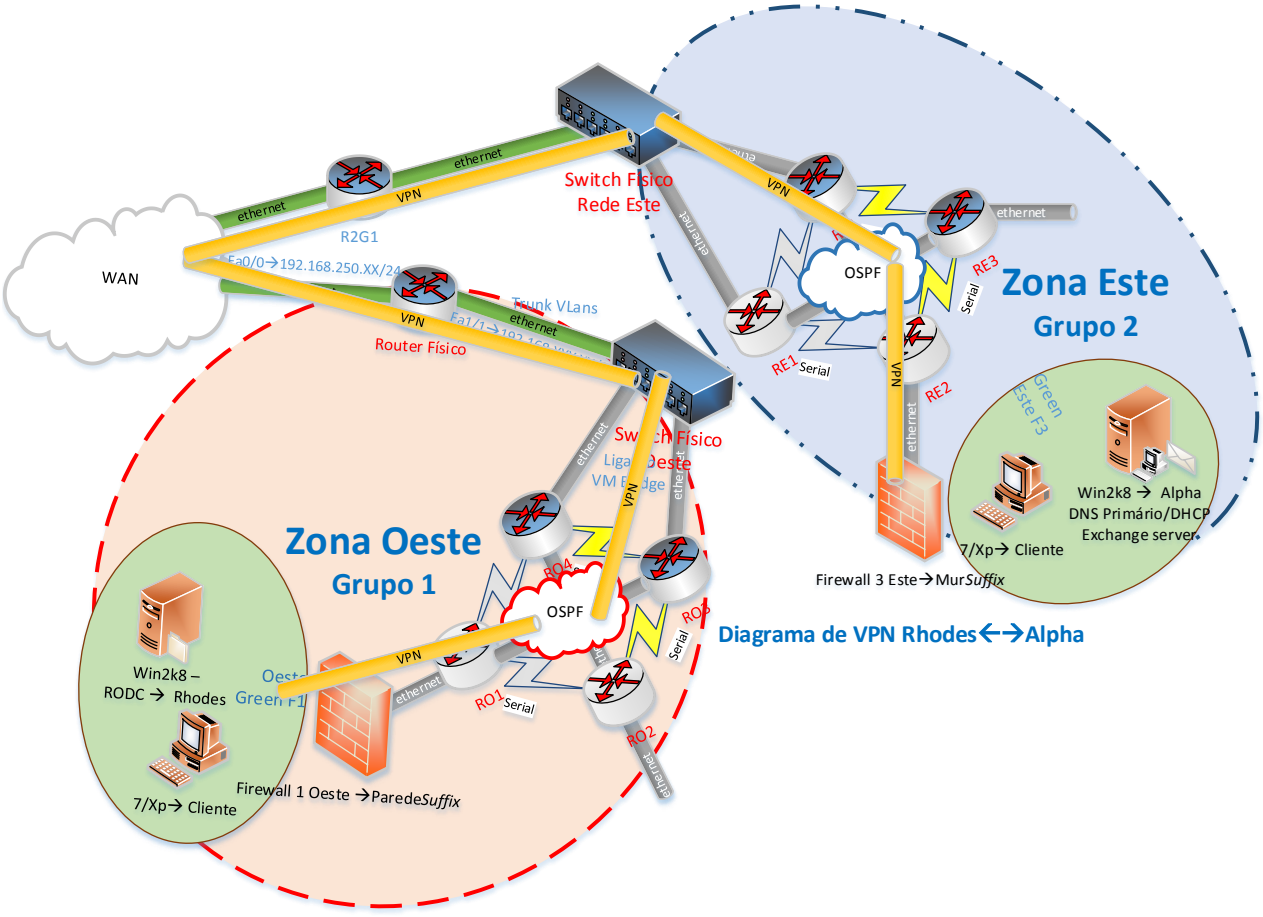


Figura 4 Diagrama VPN entre grupos (Rhodes e Alpha)

Serviços nos Firewalls

H) Todos os Firewall não devem permitir aos utilizadores aceder a sites considerados Porn, Games, Chat, Proxy redirect. Os seus hostname devem ser **ParedeSuffix**, **WallSuffix**, **MurSuffix, MuerSuffix e VeggSuffix** (ver tabela com sufixus, assim como IPs estáticos definidos para cada grupo)

H.1) Os firewall podem escolhidos da seguinte lista: Ipfire, PfSense, Smothwall, ClarkConnect, Zentyal, Endian Firewall, m0n0wall, Netdeep Cop, Shorewall, Untangle, PCX Firewall, WebCBQ Firewall, ZeroShell e IPCOP

H.2) Os utilizadores que se encontrem na Green Este Firewall **ParedeSuffix**, rede 172.16.10.X/24, devem ter acesso à internet exclusivamente no período das 09h-12h/13h-17h

H.3) Não deve permitir o acesso a páginas seguras (https), quando o pedido é efectuado da rede 172.16.10.0/24. Mas deve permitir o acesso ao correio electrónico (Gmail, Hotmail)

H.4) Não devem ter acesso a sites com TLD de domínio da Itália (.DE →Ex: www.nomesite.DE)

H.5) O acesso por SSH a qualquer um dos firewall, só deve ser permitido com a utilização de chave pública/privada. Este acesso deve ser possível de qualquer uma das interfaces que o firewall tenha.

H.6) Deve criar as ligações Site2Site entre todos os Firewall, com excepção do **MuerSuffix**: (Ver figura

H.7) Deve, igualmente, criar 4 ligações RoadWarrior (uma para cada Firewall), a utilizar por um cliente que se encontre na WAN (posicionado junto ao router físico)

H.8) Necessário a VPN (da responsabilidade do grupo que configura o **RHODES**), que ligue o **ParedeSuffix** da rede do grupo, com a firewall ESTE*suffix* do grupo com quem estão a trabalhar em conjunto. A VPN, tanto pode ser sobre OpenVPN como em IPSEC

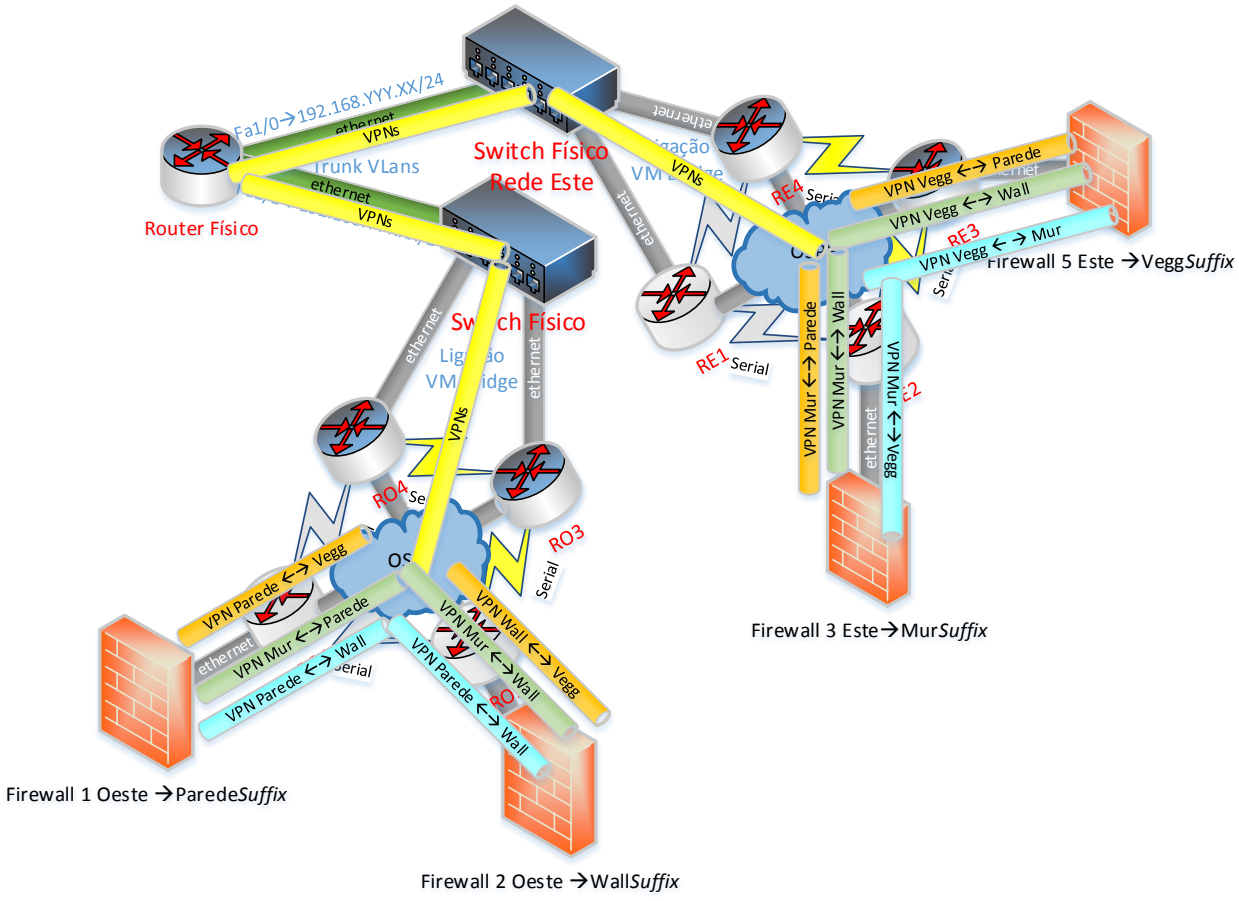


Figura 5 VPNs entre firewall

Serviços em Sigma

I) O servidor **SIGMA** funciona como o local de backup remoto para os diferentes servidores existentes na rede. Aqui também está a funcionar o serviço de monitorização de toda a rede, Nagios

I.1) O sistema deve assentar em RAID 5. Utilize discos de 1GB, para o efeito para evitar o aumento de espaço das VMs utilizadas no projecto

I.2) O relógio do servidor deve actualizar com o NTP do **YOTTA**

I.3) Para realizar os backups dos vários servidores da rede, deve de utilizar ou o serviço Amanda ou Bacula. O local para onde deve efectuar o backup, será sobre o sistema RAID

I.4) O acesso para gestão/verificação do **SIGMA** só pode ser possível da zona Green Este e Sul

I.4.1) Pode instalar uma aplicação de gestão de servidores como o Webmin ou ISPconfig **(não cotado)** para auxiliar a administração do servidor.

I.5) O servidor **SIGMA** deve ter em funcionamento um sistema de monitorização de equipamentos da rede em SNMP (Nagios/Zabbix/Zenoss)

I.5.1) O sistema que escolheu deve monitorizar

- Monitorizar todos os servidores da rede, relativamente a processador, memória, espaço em disco. Servidores:
- ALPHA (Exchange; users; serviços)
- BETA (Espaço disco; serviços; utilizadores; SSH)
- TETA → base de Dados MSsql, memoria, cpu, espaço em disco
- Rhodes →Users, memoria, cpu, espaço em disco
- DELTA, GAMA →VSFTP & PureFTP; http(Apache/Nginx; Acessos; Serviços; users)
- KSI, RHO (Espaço disco; serviços)
- YOTTA (Disco; processos; CPU,)
- PAREDE*Suffix* (Portos abertos; ligações)
- WALL*Suffix* (Portos abertos; ligações)
- MURS*uffix* (Portos abertos; ligações)
- VEGGS*uffix* (Portos abertos; ligações)
- Routers →Largura de banda disponivel nas portas, estado das portas (up/down). CPU, memória disponível, Temperatura.Deve definir os limites dos diferentes triggers dos elementos a monitorizar.
- Switch → identificação da quantidade de VLANs configuradas; estado das portas (up/down)
- Enviar uma mensagem (email) para o administrador de ALPHA.seudominio.local se algum dos parâmetros que estão a ser monitorizados atingirem valores de alerta. Esses valores, e para verificação da funcionalidade solicitada neste ponto, podem ser alterados apenas para esse fim.

Serviços nos Routers e Switch

J) Como interligação entre as redes dos diferentes projectos, e para simular uma "WAN" na sala, cada grupo terá a sua responsabilidade oito routers (vitualizados em linux – CentOS – a funcionar sobre o serviço Zebra) e router e um switch físicos (pode existir a necessidade de realizar Vlans -o switch pode ser partilhado com outro grupo). Esta interligação será desenvolvida com protocolo de roteamento, OSPF. Pretende-se igualmente redundância nas ligações, entre sistemas, e uma correcta configuração dos routers, permitirá, o roteamento dos dados de e para a WAN (no caso será a interface LAN do firewall da sala). As ligações de cada router de topo (RO4 ,RO3, RE1 e RE4) estarão em bridge com a interface da estação de trabalho onde estão a ser executados os routers virtualizados. Cada grupo terá um switch, no qual deverá configurar VLANs e ligações *trunk* , de forma a que a os seus dados possam ser correctamente diferenciados de outras ligações que o switch possa ter (um switch pode ser compartilhado por mais do que um grupo e terá de existir separação de informação gerada/recebida por qualquer dos grupos que estão ligados ao switch). Cada grupo fará uma ligação com o grupo adjunto, procurando manter – tanto quanto possivel –"Fail Over" das ligações.

J.1) Configure os routers com seis áreas de OSPF.
Redes de interligação entre routers, a sua escolha

J.2) Crie as VLANs e as ligações *trunk* necessárias para que a informação que atravessa o switch, seja diferenciável.

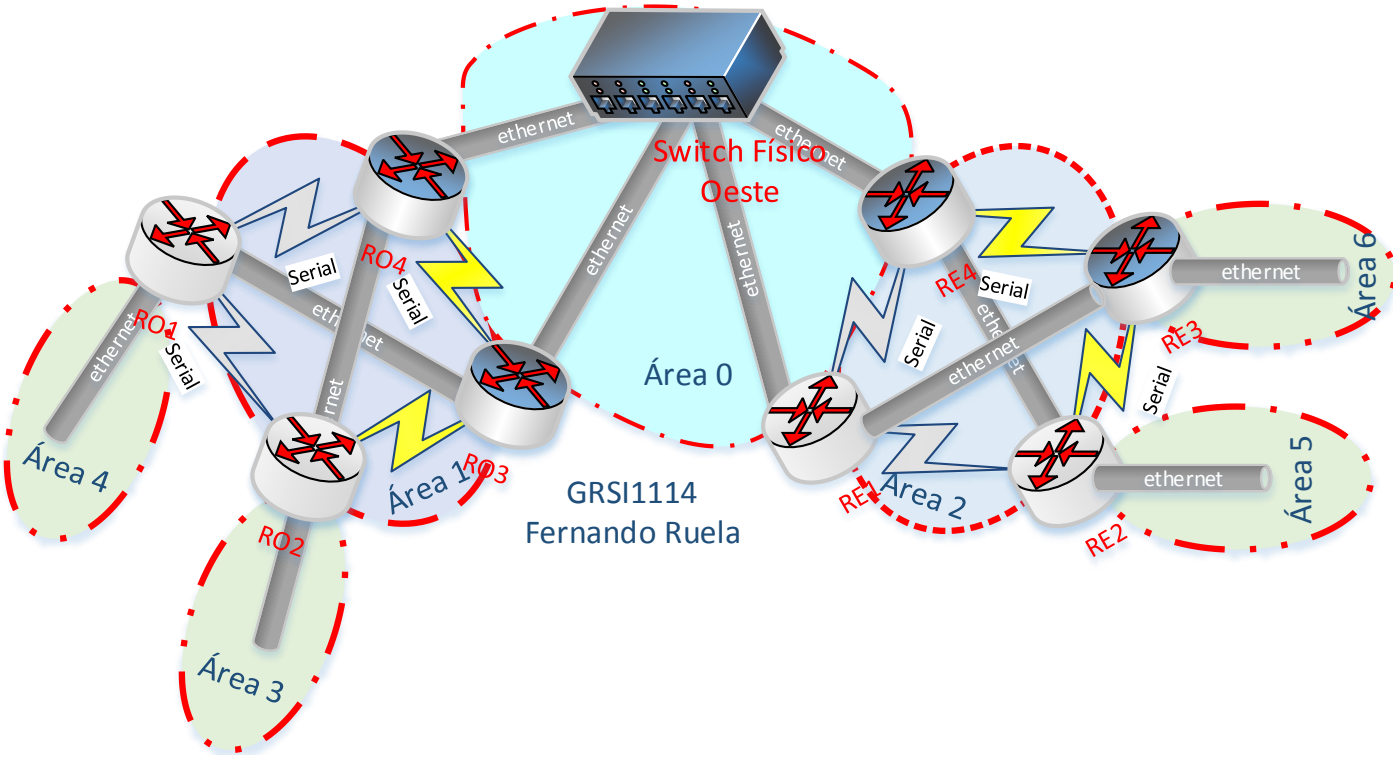


Figura 6 Áreas OSPF