UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ
CURSO TECNOLÓGICO EM REDES DE COMPUTADORES

MÁRIO FERREIRA DOS SANTOS NETO

IMPLANTAÇÃO DE UM AMBIENTE DE TESTES DE POLÍTICAS DE GERÊNCIA E SEGURANÇA PARA A EMPRESA RC2

QUIXADÁ – CEARÁ

2017

MÁRIO FERREIRA DOS SANTOS NETO

IMPLANTAÇÃO DE UM AMBIENTE DE TESTES DE POLÍTICAS DE GERÊNCIA E SEGURANÇA PARA A EMPRESA RC2

Projeto de rede apresentado no curso de Redes de Computadores na Universidade Federal do Ceará, como requisito parcial à obtenção do título de tecnólogo em Redes de Computadores. Área de concentração: Computação.

Orientador: Prof. Dr. Paulo Antonio Leal Rego.

QUIXADÁ – CEARÁ

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária

N385p Santos Neto, Mário Ferreira dos.

Implantação de um ambiente de testes de políticas de gerência e segurança para a empresa RC2 / Mário Ferreira dos Santos Neto. – 2017.
51 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Redes de Computadores, Quixadá, 2017.
Orientação: Prof. Dr. Paulo Antonio Leal Rego.

1. Redes de computadores- Projeto. 2. Infraestrutura (Economia) 3. Redes de computadores- Gerência. I. Título.

CDD 004.6

MÁRIO FERREIRA DOS SANTOS NETO

IMPLANTAÇÃO DE UM AMBIENTE DE TESTES DE POLÍTICAS DE GERÊNCIA E SEGURANÇA PARA A EMPRESA RC2

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Redes de Computadores da Universidade Federal do Ceará, como requisito parcial à obtenção do título de tecnólogo em Redes de Computadores.

Área de concentração: Computação.

Aprovado em:_____/_____/_____.

BANCA EXAMINADORA

_____
Prof. Dr. Paulo Antonio Leal Rego (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Me. Jeandro de Mesquita Bezerra
Universidade Federal do Ceará (UFC)

_____
Prof. Me. Michel Sales Bonfim
Universidade Federal do Ceará (UFC)

Aos meus familiares, a minha companheira, aos meus amigos, aos colegas de trabalho, e a todos aqueles que acreditaram em mim.

AGRADECIMENTOS

Ao professor Paulo Rego pela orientação deste projeto e disposição em me auxiliar ao longo desse período trabalhando juntos, sempre com muito compromisso e profissionalismo.

Aos meus companheiros de trabalho Renzo Megli e Tiago Oliveira pelos inúmeros conselhos, apoio e suporte técnico necessário para conclusão e sucesso desse projeto.

Ao meu primo Wellington Matheus por ter acreditado em mim e ser um dos grandes responsáveis pela minha motivação na reta final do curso.

A minha companheira de vida, Maressa Ferreira, pelo apoio incondicional nos meus momentos mais difíceis.

À minha família, pilar e espelho para a pessoa que sou hoje.

Aos colegas de turma que conviveram comigo nesta trajetória, especialmente Jeyvison, Samuel, Otávio, Pedro e Rodrigo.

Aos demais que não foram citados nominalmente, mas que proporcionaram grandes momentos que irei sempre recordar.

RESUMO

O contínuo crescimento da tecnologia da informação, especialmente nas áreas de infraestrutura e segurança da informação, vem exigindo cada vez mais serviços com alta disponibilidade, desempenho e segurança das empresas prestadoras. Muitas delas buscam consolidar parcerias com grandes fabricantes mundiais para oferecerem excelência em seus produtos e serviços, sempre buscando atender a gama de necessidades de seus clientes. Além disso, o treinamento e aprimoramento técnico da equipe operacional é muito importante nesse modelo de negócio. Por isso, uma das alternativas para o crescimento profissional é a oferta de um ambiente de testes para que esses profissionais possam realizar atividades voltadas a testes, estudos, simulações e outras atividades sem provocar impactos no ambiente operacional da empresa. Com base nesse princípio, esse projeto mostra o processo de implantação de um ambiente de testes de políticas de gerência e segurança para a empresa RC2. O projeto foca na implementação das ferramentas e soluções de segurança mais utilizadas na empresa, com o intuito de ampliar o conhecimento teórico e técnico da equipe operacional, além de auxiliar no processo e fluxo de atendimento aos clientes. Ao término da implantação e execução desse projeto, muitos resultados positivos foram obtidos, o que garantiu a aprovação tanto da gestão, para manutenção do ambiente, quanto dos clientes através de *feedbacks* positivos e demandas atendidas com sucesso.

Palavras-chave: Projeto de Rede. Segurança da Informação. Infraestrutura. Gerenciamento de Rede.

ABSTRACT

The continuous growth of information technology, mainly in the infrastructure and information security area, is increasingly demanding services with high availability, performance and security from its providers. Many of these providers seek to consolidate partnerships with world's largest manufacturing companies in order to offer excellence on products and services, searching to fulfill the range of their customers' needs. In addition, the training and technical improvement of the operational team are crucial in this business model. Therefore, one of the alternatives for professional growth is the offer of a testing environment so that these professionals can perform activities focused on tests, studies, simulations and other activities without causing impacts in the operating environment of the company. Based on this principle, this project shows the process of deploying a management and security policy testing environment for the RC2 company. The project focuses on the implementation of the most used security tools and solutions in the company, with the aim of increasing the theoretical and technical knowledge of the operational team, as well as assisting in the procedures and flow of customer service. At the end of the implementation and execution of this project, many positive results were acquired, which guaranteed the approval of both IT manager, for the maintenance of this environment, and the clients through positive feedbacks and demands that were successfully met.

Keywords: Network Design. Information Security. Infrastructure. Network Management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

NOC	Network Operations Center
LAN	Local Area Network
WAN	Wide Area Network
ISO	International Organization for Standardization
TMN	Telecommunications Management Network
DDoS	Distributed Denial of Service
SNMP	Simple Network Management Protocol
MIB	Management Information Base
DoS	Denial of Service
TCP	Transmission Control Protocol
HTTPS	Hyper Text Transfer Protocol Secure
FTP	File Transfer Protocol
SSH	Secure Shell
IP	Internet Protocol
IKE	Internet Key Exchange
DHCP	Dynamic Host Configuration Protocol
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
UTP	Unshielded Twisted Pair
WMI	Windows Management Instrumentation
SMTP	Simple Mail Transfer Protocol
POP	Post Office Protocol
CPU	Central Processing Unit
UTM	Unified Threat Management
SSL	Secure Sockets Layer
IPS	Intrusion Prevention System
Gbps	Gigabit per seconds
MPLS	Multiprotocol Label Switching

SUMÁRIO

1 INTRODUÇÃO

A RC2 (por questões de sigilo, um nome fantasia é utilizado neste trabalho) é uma empresa prestadora de serviços gerenciados e integradora de soluções em *datacenter*, infraestrutura e segurança da informação. Com sede na cidade de Fortaleza e atuando em todo o Brasil, possui duas equipes técnicas: uma dedicada à implantação, onde são levantados os requisitos e necessidades dos clientes até a implementação da solução, e outra equipe dedicada à operação, atuando em ambiente operacional, conhecido como NOC (*Network Operation Center* ou Centro de Operação de Rede), para gerenciamento das soluções implantadas em tempo real.

Nos últimos anos, houve um aumento expressivo na demanda de soluções voltadas à f*irewalls* de nova geração e monitoramento de ativos de rede com detecção minuciosa de incidentes, capazes de oferecerem relatorias que atendam às mais diversas necessidades dos clientes. Entre as soluções de f*irewall* ofertadas, SonicWall[1] e Sophos[2] destacam-se pela robustez e a variedade de recursos e funcionalidades em seus equipamentos, possibilitando uma segurança abrangente com um gerenciamento eficiente e escalável. Quanto à solução de monitoramento, a RC2 utiliza a ferramenta PRTG Network Monitor[3], classificada como uma das melhores ferramentas de monitoramento de rede pela revista TechRadar (2017). Embora ambas as soluções possuam documentação e treinamento técnico oferecido pela RC2, o contato direto é necessário para o completo domínio delas, seguindo também um processo de segurança para evitar que o momento de aprendizado não cause impactos no ambiente operacional.

Diante desse cenário, onde se busca e exige expertise nas soluções de segurança sem utilizar dos equipamentos em produção, um ambiente de testes é primordial para que qualquer ação voltada a testes, aprimoramento técnico e demais atividades relacionadas às soluções possam ser atendidas de maneira objetiva e segura. O apoio da gestão na autorização da elaboração e execução do projeto, disponibilizando todos os recursos também é fundamental nesse processo.

Portanto, com a implantação desse ambiente, além das possibilidades citadas, o processo de transição para futuros membros da equipe técnica também será beneficiado, de modo que a familiarização com as soluções seja a mais rápida possível.

[1] https://www.sonicwall.com/en-us/products/firewalls
[2] https://www.sophos.com/en-us/products/next-gen-firewall.aspx
[3] https://www.paessler.com/prtg

2 OBJETIVO DO PROJETO

Este projeto tem como objetivo desenvolver um ambiente de testes de políticas de gerência e segurança para a empresa RC2, disponibilizando acesso aos *firewalls* SonicWall e Sophos, bem como ao sistema de monitoramento PRTG – licenciados-, para realização de testes, simulações, integrações, estudos e demais atividades práticas. Essa implantação visa ampliar os conhecimentos teóricos e técnicos das ferramentas, permitindo que a equipe de suporte tenha uma maior expertise quanto às ações relativas à suporte, incidentes e demandas diversas, além de otimizar os atendimentos realizados. Além disso, o projeto também busca uma redução de custos relacionados a treinamento e repasses técnicos, muitas vezes realizados fora do expediente de trabalho.

3 ESCOPO DO PROJETO

O escopo do projeto é implantar um ambiente de testes de políticas de gerência e segurança na empresa, disponibilizando para a equipe técnica as ferramentas necessárias para a realização de atividades voltadas à segurança, conectividade, infraestrutura, gerenciamento e monitoramento de rede. Fisicamente, a rede será integrada ao ambiente operacional do NOC, utilizando do espaço compartilhado. Topologicamente, fará parte de uma nova zona, isolada, da rede LAN da operação. O ambiente incluirá todos os equipamentos de rede necessários para a plena execução das atividades mencionadas. Esses equipamentos serão detalhados no Projeto Físico.

Não faz parte do escopo do projeto a escolha do endereçamento WAN dos equipamentos e o *link* de saída para a internet. A aquisição das licenças dos equipamentos também não faz parte do projeto, sendo elas já repassadas pela gestão.

4 CONCEITOS

Para um entendimento apropriado do projeto, torna-se necessária a abordagem de dois conceitos que são os pilares de seu desenvolvimento: gerenciamento de rede e segurança da informação.

4.1 Gerenciamento de rede

PINHEIRO (2006) define gerenciamento de rede como "O controle de atividades e monitoração de uso de recursos materiais e/ou lógicos, fisicamente distribuídos na rede, buscando a confiabilidade, tempos de resposta aceitáveis e segurança das informações". Seu modelo pode ser dividido em três etapas bem definidas, pelo qual inicia-se através do processo de monitoramento dos recursos gerenciados, chamado de coleta de dados. O segundo passo consiste no tratamento e análise destes dados coletados, conhecido como diagnóstico. Por fim, o modelo do gerenciamento de rede dispõe da ação e controle dos recursos gerenciados, estando presentes na solução ou prevenção de possíveis incidentes.

CLEMM (2007) também relaciona o gerenciamento de redes em cinco áreas funcionais, sendo elas Gerenciamento de Falhas, Gerenciamento de Configuração, Gerenciamento de Contabilidade, Gerenciamento de Desempenho, e Gerencioamento de Segurança. Elas são estabelecidas pela ISO *(International Organization for Standardization)* e seguidas pelo modelo de gerenciamento TMN *(Telecommunications Management Network)*. A seguir, serão detalhadas essas áreas:

Gerenciamento de falhas

O gerenciamento de falhas lida com falhas ocorridas na rede, sejam elas de equipamento ou *software*. Leva em questão o monitoramento do estado dos recursos da rede para garantir que tudo esteja operando de maneira adequada e agir de imediato em caso de uma condição anormal. Um gerenciamento de falhas efetivo é crucial para garantir que os usuários não presenciem uma interrupção de serviço, e caso aconteça, tal interrupção seja minimizada.

Gerenciamento de configuração

O gerenciamento de configuração consiste no processo de reunir e armazenar informações dos dispositivos da rede. Uma rede dificilmente permanece estática por muito tempo, ou seja, haverá a necessidade de reparo, de adição ou remoção de dispositivos ou até mesmo de uma expansão. Então, com o banco de dados concentrando essas informações é

possível determinar o melhor caminho para tais ações. As informações armazenadas podem ser sobre localizações e endereços de rede dos dispositivos, aplicações, versões e atualizações instaladas e configurações gerais de dispositivos.

Gerenciamento de contabilidade

O gerenciamento de contabilidade consiste na coleta de estatísticas de utilização dos recursos da rede. Seu objetivo é garantir que esses recursos sejam utilizados de maneira satisfatória por todos os usuários e, quando aplicável, regular a utilização dos mesmos. O gerenciamento de contabilidade também engloba o gerenciamento de administração, que estabelece usuários, senhas e permissões de acesso à rede.

Gerenciamento de desempenho

O gerenciamento de desempenho lida com o monitoramento e melhoria da performance da rede. Isto é, diferentes indicadores de desempenho, como taxa de transmissão, latência e vazão de dados são coletados constantemente e comparados a níveis predeterminados, ou limites. A excedência desses limites é indicativo de anormalidades que precisam de atenção por parte do gerente. Após isso, esforços devem ser atribuídos para identificar quais melhorias podem ser realizadas para contribuir com o desempenho geral da rede.

Gerenciamento de segurança

O gerenciamento de segurança envolve os aspectos relacionados à proteção da rede. Protegê-la de ameaças como ataques *hackers*, ataques de negação de serviço (DDoS - D*istributed Denial-of-Service*), propagação de vírus e spam e tentativas de intrusão é um objetivo crucial. Além disso, o gerenciamento de segurança também engloba a segurança física, ou seja, inclui mecanismos de controle de acesso aos equipamentos e servidores da rede.

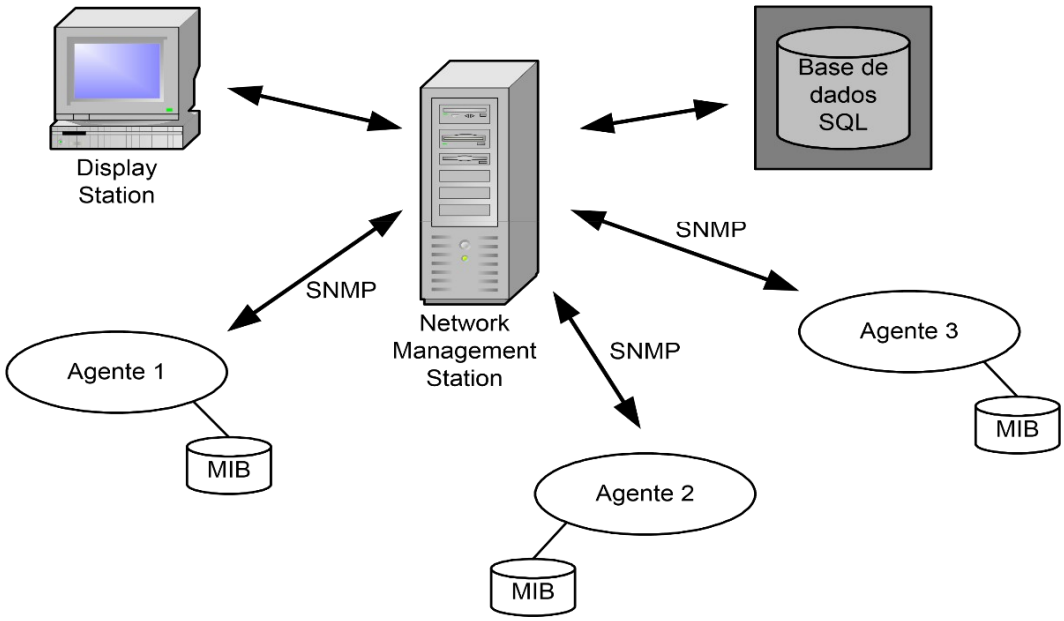
4.1.1 SNMP

No decorrer da descrição das áreas funcionais do gerenciamento de redes, foi unanimidade a menção de coleta de dados e monitoramento dos dispositivos da rede para fins diversos. Esta é a função do SNMP. O SNMP (*Simple Network Management Protocol*) é o protocolo padrão para gerenciar e monitorar dispositivos em uma rede de maneira simplificada e em tempo real. Foi criado em 1989 diante da necessidade de um padrão de

gerenciamento de dispositivos IP (*Internet Protocol*) e teve sua primeira versão publicada em 1990 e atualmente está na versão 3.

O SNMP é baseado no conceito de agentes e gerentes. O agente é um *software* existente nos dispositivos gerenciáveis da rede (roteadores, *switches*, computadores, etc.) responsável pela coleta e envio de dados a um gerente. O gerente é o responsável por executar as funções de gerenciamento, ou seja, é quem solicita a coleta dos dados para análise e monitoramento. Os dados coletados pelo agente são armazenados em um banco de dados lógico conhecido como MIB (*Management Information Base*). A figura 1 ilustra o funcionamento do SNMP:

Figura 1 – Estrutura de gerenciamento SNMP



Fonte: Teleco (2012)

Nesse projeto, o SNMP é utilizado majoritariamente no PRTG. Todos os ativos gerenciados pela RC2 oferecem suporte a esse protocolo, então mecanismos otimizados para gerência, estudo das MIBs dos equipamentos e criação de sensores e *templates* customizados na ferramenta serão requisitados para o contínuo aprimoramento das atividades de monitoramento da empresa.

4.2 Segurança da informação

A questão da segurança sempre foi uma das maiores preocupações da sociedade ao longo das décadas, seja ela relacionada à segurança doméstica, pública ou privada. Com a segurança da informação não é diferente, uma vez que, com os avanços da informática e o monopólio cada vez maior de informações armazenadas no meio virtual, torna-se imprescindível os meios para que estas informações estejam sempre seguras.

De acordo com CHERDANTSEVA; HILTON (2014), a segurança da informação pode ser descrita como uma área multidisciplinar de estudo e de atividade profissional, pela qual existe a importância do desenvolvimento e implementação dos mais variados métodos a fim de garantir que a informação e os sistemas de informação - onde as informações são criadas, processadas, armazenadas e/ou destruídas -, estejam livres de roubo, espionagem, modificação e outras ameaças.

BRAUMANN, CAVIN e SCHMID (2011) dividem a segurança da informação em três princípios básicos, conhecidos como *CIA Triad*, ou Tríade CID: Confidencialidade, Integridade e Disponibilidade, conforme ilustrado na Figura 2.

Figura 2 - Tríade CID

Fonte: PORTELLA, MONTEIRO, MOREIRA (2012)

Confidencialidade

É um conceito no qual o acesso à informação, esteja ela armazenada, em processamento ou em trânsito não deve ser concedido a sujeitos não autorizados, ou seja, apenas aqueles com direitos e privilégios devem acessá-la. Ataques à confidencialidade podem ser através da escuta, também conhecida como análise de tráfego. Um ataque de escuta é atribuído geralmente à interceptação de dados. Para evitar esse tipo de ataque, técnicas de criptografia são utilizadas para tornar os dados incompreensíveis ao interceptador.

Integridade

O conceito de integridade refere-se a garantia de que a informação não tenha sido alterada durante as fases de transmissão e recepção. BRAUMANN, CAVIN e SCHMID (2011) apontam duas categorias de integridade: integridade de fonte e integridade de dados. A integridade de

fonte garante que os dados estão realmente vindo do emissário correto, enquanto a integridade de dados refere-se a garantia de que os dados não foram manipulados, intencionalmente ou acidentalmente antes de serem lidos pelo destinatário pretendido. Ataques à integridade podem ser realizados através da modificação, falsificação, repetição ou retratação dos dados. Uma estratégia de defesa muito comum é a utilização de criptografia para comunicações seguras.

Disponibilidade

O terceiro componente da segurança da informação é a disponibilidade. O conceito de disponibilidade significa que a informação ou os recursos devem estar sempre disponíveis para uso quando usuários autorizados os requisitam. Ataques à disponibilidade são geralmente através da negação de serviço (DoS – *Denial of Service*), capazes de reduzir a velocidade ou até mesmo interromper completamente um serviço. É um dos problemas mais crescentes entre as empresas nos últimos anos, requerendo uma atenção especial para infraestrutura e novas tecnologias.

Baseando-se então nesses 3 princípios, é importante observar as tendências e os desafios a serem enfrentados nessa área. De acordo com o último relatório anual de ameaças da SonicWall (2017), houve um avanço de crimes cibernéticos nas categorias de *ransomware* - código malicioso capaz de criptografar os dados de usuários e se auto replicar dentro de uma rede, exigindo pagamento de um resgaste para descriptografar esses dados-, e ataques DDoS (*Distributed DoS*), que comprometeram dispositivos em larga escala principalmente nos Estados Unidos, Brasil e Índia. Por isso, o pleno conhecimento das boas práticas e funcionalidades das soluções de segurança são indispensáveis para que incidentes desse tipo não ocorram na infraestrutura dos clientes.

5 REQUISITOS DE PROJETO

Nesta seção, são apresentados os requisitos do projeto, divididos em objetivos de negócio e objetivos técnicos.

5.1 Objetivos de Negócio

- Ampliar a expertise da equipe de suporte quanto à utilização das ferramentas e suas funcionalidades;
- Auxiliar na capacitação de novos colaboradores, de modo que esses possam se adaptar rapidamente as soluções, caso não sejam familiarizados;
- Reduzir o tempo de resposta no tratamento de incidentes;
- Garantir que as tomadas de ações nos atendimentos sejam efetivas e não causem impactos na produção do cliente, através de testes preliminares;
- Redução de custos com treinamento e repasses técnicos.

5.2 Objetivos Técnicos

- **Escalabilidade**

  A escalabilidade refere-se à capacidade de crescimento da rede, ou seja, como a rede pode suportar um número crescente de novos usuários sem impactar em novos custos, como aquisição de novos equipamentos. Se tratando apenas de um ambiente de testes, não há expectativas de expansão por pelo menos 2 anos. No entanto, existem planejamentos em execução para ampliação do NOC e da comunidade de usuários, então a possibilidade de um crescimento, mesmo que mínimo, não deve ser descartada.

- **Disponibilidade**

  Embora os usuários do ambiente necessitem de sua disponibilidade sempre que possível, uma alta disponibilidade não pode ser garantida em virtude de várias interrupções que podem ocorrer durante execuções de testes e outras atividades. Portanto, esse objetivo técnico não é prioridade do projeto, uma vez que indisponibilidades de até mesmo dias poderão ser observadas.

- **Desempenho**

  Os usuários do ambiente estarão constantemente realizando testes, atualizações e simulações que podem estressar os equipamentos e o enlace da rede. Então, utilizar da capacidade de transmissão de pelo menos 100Mbps e uma latência inferior a 50ms são importantes para essas atividades operarem de maneira satisfatória.

- **Segurança**

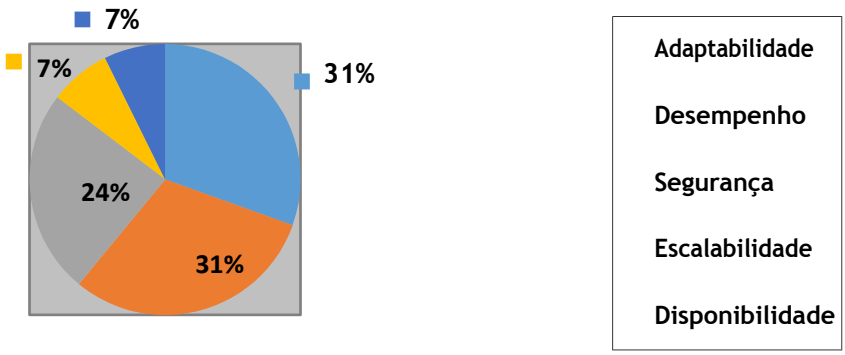
  Aspecto muito importante. Devido a alterações constantes que serão realizadas, o ambiente de testes necessita estar completamente isolado da rede LAN da RC2. Além disso, embora seja apenas um ambiente de testes, acessos não autorizados precisam ser evitados, seja no meio virtual como presencial.

- **Adaptabilidade**

  Finalmente, o ambiente precisa ter capacidade para se adaptar às novas mudanças. Sejam elas mudanças de tecnologia, protocolos, formas de negócio ou legislação. Entre essas mudanças, a está em planejamento a integração do Firewall Checkpoint e gerência dos antivírus Kaspersky e Sophos, também para testes.

No gráfico abaixo estão divididas as prioridades para a rede, baseadas em um consenso da equipe operacional da RC2:

Figura 3: *Tradeoff* de objetivos da rede



Fonte: Elaborado pelo autor (2017)

5.3 Comunidades de Usuários e Armazenadores de Dados

Nas tabelas a seguir, estão detalhadas as comunidades de usuários e armazenadores de dados da rede.

5.3.1 Comunidades de Usuários

A comunidade de usuários corresponde a um conjunto de usuários na rede que utilizam as mesmas aplicações, dividido por departamentos. Foram documentadas as comunidades de acordo com a Tabela 1:

Tabela 1: Comunidade de usuários

Nome da Comunidade	Tamanho da Comunidade	Localização da Comunidade	Soluções utilizadas
Monitoramento – Equipe responsável pelo monitoramento de soluções de segurança e ambiente de infraestrutura.	6	NOC	PRTG; Windows Server; Ubuntu.
Nível 1 – Equipe de suporte de primeiro nível, atendimento a clientes em horário comercial.	3	NOC	Sophos; SonicWall; Aruba; Mikrotik. Windows Server; Ubuntu.
Nível 2 – Equipe de suporte de segundo nível, responsável por atendimentos escalonados do nível 1, atendimento a clientes *VIPs* e 24x7.	4	NOC	Sophos; SonicWall; Aruba; Mikrotik. Windows Server; Ubuntu.
Nível 3 – Equipe de suporte de terceiro nível, responsável por atendimentos escalonados do nível 2, visitas a infraestrutura de clientes e atuação em ambientes complexos.	2	NOC	Sophos; SonicWall; Aruba; Mikrotik. Windows Server; Ubuntu.

Supervisão – Responsável pelo acompanhamento da equipe e gerenciamento dos atendimentos.	1	NOC	PRTG; Windows Server.

Fonte: Elaborado pelo autor (2017)

5.3.2 Armazenadores de dados

Os armazenadores de dados são equipamentos que armazenam dados que são utilizados por aplicações na rede. Foi documentado o armazenador conforme a Tabela 2:

Tabela 2: Armazenadores de Dados

Tipo de armazenador de dados	Quantidade	Localização	Comunidades utilizadoras	Aplicações
Servidor de testes	1	NOC	Monitoramento, Nível 1, Nível 2, Nível 3 e Supervisão.	PRTG.

Fonte: Elaborado pelo autor (2017)

5.4 Aplicações de Rede

A Tabela 3 apresenta as aplicações de rede, que poderão ser utilizadas por toda a comunidade de usuários. O PRTG está instalado diretamente no servidor de testes, permitindo a modificação dos arquivos de configuração para aprimoramento e descobertas de sensores que facilitem a gerência dos ativos de produção sem qualquer interferência no ambiente externo. Já as demais aplicações são destinadas ao gerencialmente dos *firewalls* e podem ser utilizadas fora do servidor através dos IPs de WAN, ou também na própria rede interna do ambiente.

Tabela 3: Aplicações de rede

Aplicação	Criticidade	Nova aplicação	Tipo de Fluxo de Tráfego	Protocolos utilizados	Comunidade Utilizadora	Armazenamento de dados	Requisito aprox. de dados
PRTG	Alta	SIM	Cliente/ Servidor	TCP, HTTPS	Todos	Servidor	1Mbps
VPN Client	Baixa	SIM	Cliente/ Servidor	IKE, DHCP, IP, TCP	Todos	N/A	N/A

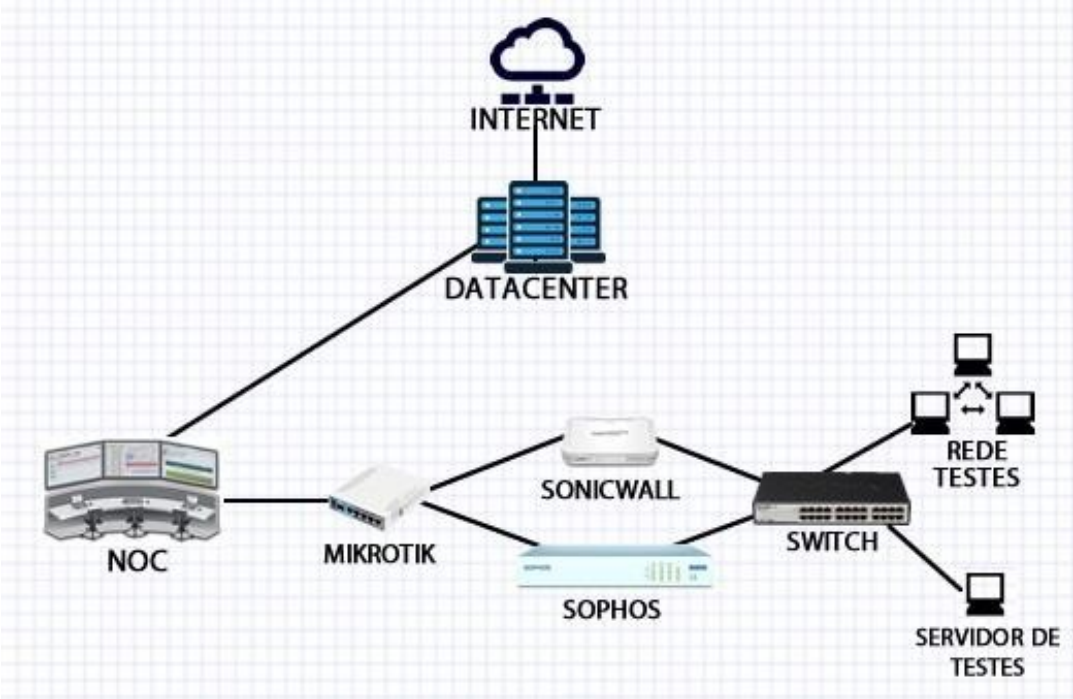
Fonte: Elaborado pelo autor (2017)

6 PROJETO LÓGICO DA REDE

6.1 Topologia da rede

O ambiente de testes está topologicamente projetado de acordo com a Figura 4.

Figura 4: Esquema da rede proposta



Fonte: Elaborado pelo autor (2017)

A topologia está projetada de maneira hierárquica, com o Mikrotik em modo *bridge* atuando como ponto central da rede, responsável por garantir a conectividade dos equipamentos. Os *firewalls* estão isolados através de VLANs (*Virtual Local Area Network*), de modo que testes simultâneos nas duas soluções não colidam e interfiram entre si. Essas VLANs estarão configuradas em um *switch*, que irá comportar o servidor e demais hosts utilizados para testes no ambiente. A VLAN a ser utilizada pelo servidor e os outros hosts ficará a critério do usuário, com intervenção manual no cabeamento para saída de internet através do Sophos, SonicWall, Aruba ou diretamente para a internet pelo Mikrotik.

6.2 Endereçamento

A rede será segmentada em 3 VLANs para isolar os ambientes das soluções, com o mínimo de tráfego de broadcast e realizando boas práticas para evitar desperdício de IPs, mesmo em uma rede local. A Tabela 4 documenta o esquema de endereçamento dos hosts, descrevendo as faixas de IPs, a quais VLANs pertencem e onde serão utilizadas:

Tabela 4: Endereçamentos

VLAN ID	SUBREDE	END. REDE	END. BROADCAST	PRIM. MAQ. (GATEWAY)	ULT. MAQ.	TOTAL HOTS	OBS
VLAN_100 Gerência do Switch	192.168.1.0/28	192.168.1.0	192.168.1.15	192.168.1.1	192.168.1.14	14	*Switch*.
VLAN_10	192.168.10.0/28	192.168.10.0	192.168.10.15	192.168.10.1	192.168.10.14	14	SonicWall.
VLAN_20	192.168.20.0/28	192.168.20.0	192.168.20.15	192.168.20.1	192.168.20.14	14	Sophos.

Fonte: Elaborado pelo autor (2017)

Será utilizado o endereçamento dinâmico (DHCP) nos hosts, porém alguns dispositivos necessitam de um endereço IP já definido, ou seja, com endereço estático. A Tabela 5 documenta os dispositivos com IP estático.

Tabela 5: Endereçamento estático

Nome	Endereço IP
SWITCH	192.168.1.1
SONICWALL_WAN	192.168.2.83
SOPHOS_WAN	192.168.2.84
SONICWALL_LAN	192.168.10.1
SOPHOS_LAN	192.168.20.1

Fonte: Elaborado pelo autor (2017)

6.3 Nomenclaturas

Foram criados os seguintes identificadores para auxiliar na identificação dos equipamentos distribuídos na rede:

Tabela 6: Esquema de nomes

Dispositivo	**Nomenclatura**
Servidor de testes	SRV
Switch	SWITCH
SonicWall	SONICWALL
Sophos	SOPHOS
Aruba	AP

Fonte: Elaborado pelo autor (2017)

6.4 Protocolos

A conectividade básica entre os equipamentos não utilizará roteamento, apenas comutação. Por isso, a seleção de protocolos de rede utilizados é breve, conforme na listagem abaixo:

- IEEE 802.1Q: protocolo necessário para a criação e comunicação de VLANs na rede, mesmo em *switches* diferentes;
- *Layer* 2 *switching*: protocolo padrão do *switch* da rede, utilizado para comunicação baseado em endereços MAC.

6.5 Soluções

A seguir são apresentadas com maiores detalhes as soluções a serem implementadas no ambiente de testes.

6.5.1 PRTG Network Monitor

O PRTG[4] é um *software* de monitoramento de rede capaz de coletar informações e estatísticas de qualquer ativo dentro de uma rede, como roteadores, servidores físicos e virtuais, *switches*, *firewalls*, aplicações e até sistemas de controle de temperatura para datacenters. Além

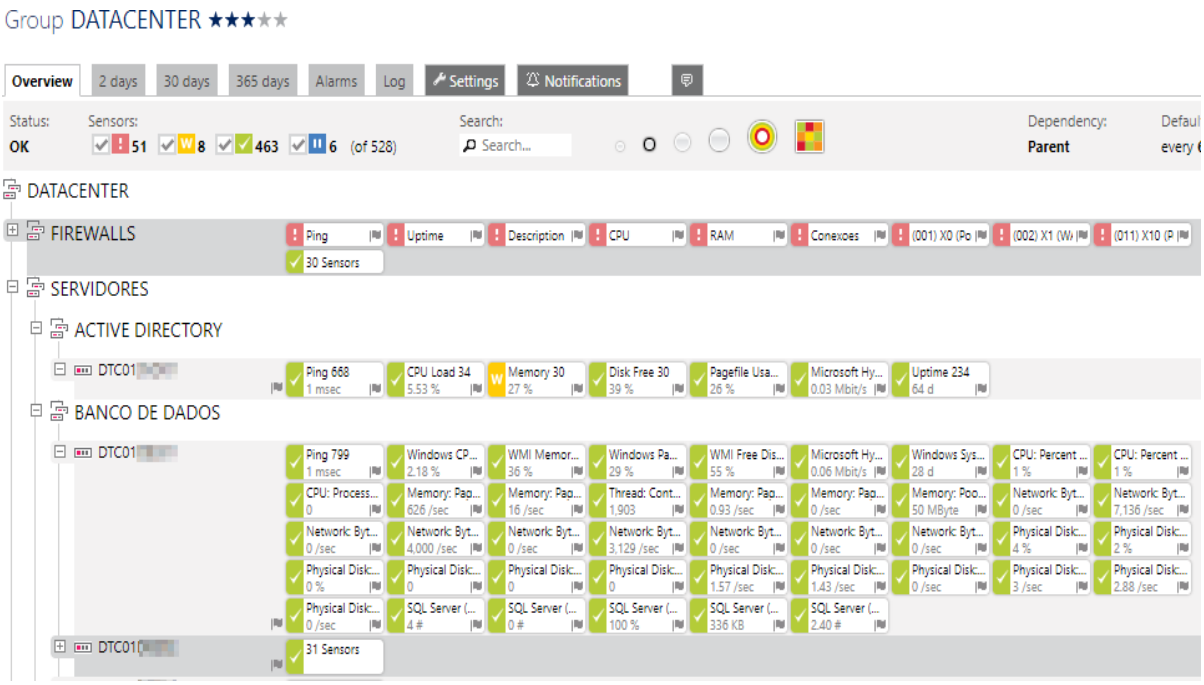
[4] https://www.paessler.com/prtg

de toda essa abrangência de monitoramento, a capacidade de descoberta e autoconfiguração e de novos ativos utilizando *templates* dos principais fabricantes permite uma gerência altamente intuitiva e facilitada. A ferramenta também oferece suporte a notificações remotas, permitindo o administrador da rede a receber alertas para qualquer evento via *E-mail*, SMS, WhatsApp e Telegram.

A maneira que o PRTG trabalha é através da utilização de sensores, que são objetos de monitoramento individuais configurados para um propósito específico. Por exemplo, existem sensores do tipo Ping, SNMP, WMI, SSH, HTTP, SMTP/POP3 (Email), além de sensores específicos de *hardware* para *switches*, roteadores e servidores, como sensores que acompanham o status de uma interface de rede. O PRTG possui mais de 200 sensores pré-configurados que obtém estatísticas de ativos monitorados, como tempos de resposta e utilização de memória, CPU e banda.

O PRTG é uma das aplicações mais críticas no ambiente da RC2, pois toda a infraestrutura interna e de seus clientes são monitoradas através dessa ferramenta. Com isso, torna-se completamente inviável a utilização do PRTG em produção para execução de atividades com fins de testes. Qualquer configuração equivocada pode causar impactos imensuráveis. Portanto, outra aplicação do PRTG instalada no servidor de testes é uma alternativa para que essas atividades sejam realizadas de maneira segura.

Figura 5 – *Dashboard* PRTG



Fonte: Elaborado pelo autor (2017)

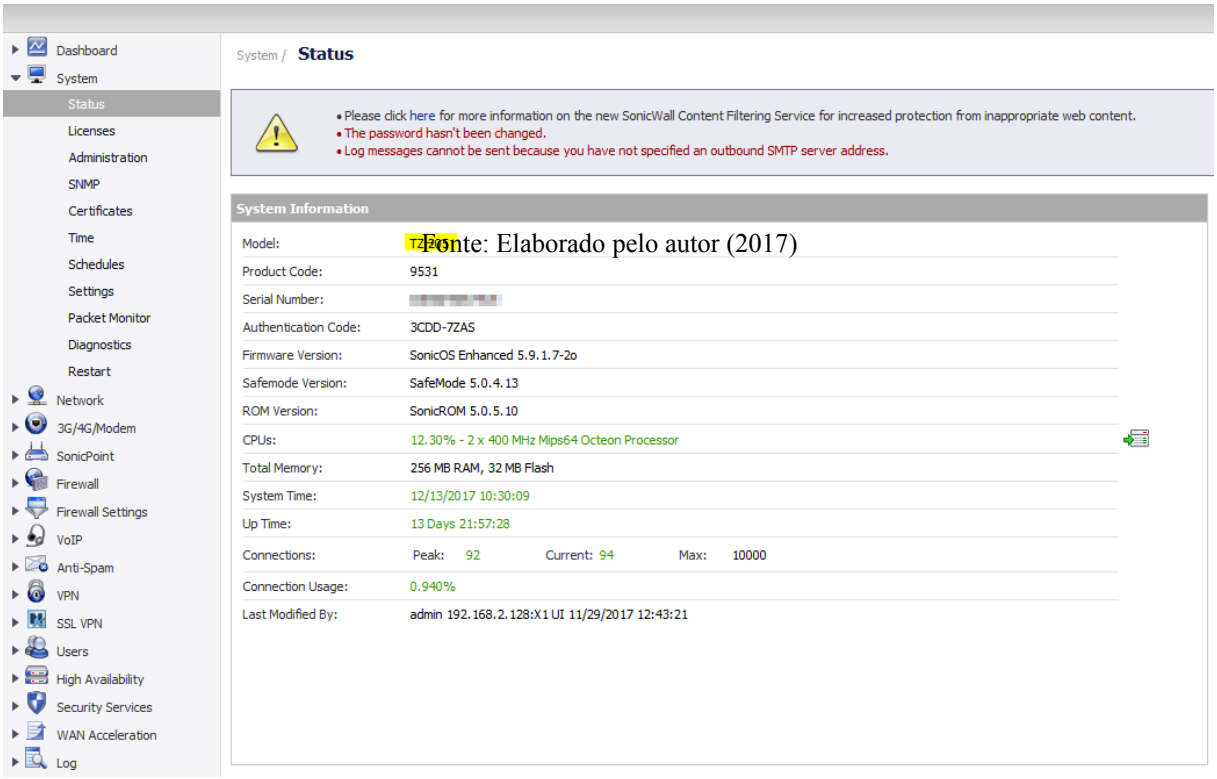
6.5.2 **SonicWall**

A SonicWall é uma empresa americana fundada em 1991, subsidiada pela Dell entre 2012 e 2016, entre as líderes no mercado de segurança para pequenas e médias redes. Ela provê serviços e equipamentos como firewalls UTM (*Unified Threat Management* – Gerenciamento unificado de ameaças), VPN (*Virtual Private Network*) e *anti-spam* para e-mail.

Os equipamentos SonicWall integram as principais funções de segurança de perímetro incluindo Firewall, VPN IPsec e SSL, IPS, Filtro de Conteúdo *Web*, *Geo* IP *filter*, *Botnet Filter*, Antivírus e Anti-*spyware* de *gateway*. Além disso, permite integração com *Active Directory* e com redes *wireless* seguras. Também dispõe de recursos para balanceamento e otimização de links.

A RC2 possui aproximadamente 2/3 de clientes que possuem f*irewalls*, utilizando as soluções SonicWall. No entanto, não existe uma documentação facilmente disponível na internet, além do treinamento técnico depender de fatores como compra de vouchers que disponibilizam ao usuário o acesso ao ambiente de treinamento. Dessa forma, a disponibilização de um *firewall* SonicWall, cuja especificação técnica está disponível no Anexo A, para o ambiente possui um enorme benefício para toda a equipe técnica, em virtude de uma logística burocrática.

Figura 6 – Dashboard SonicWall



Fonte: Elaborado pelo autor (2017)

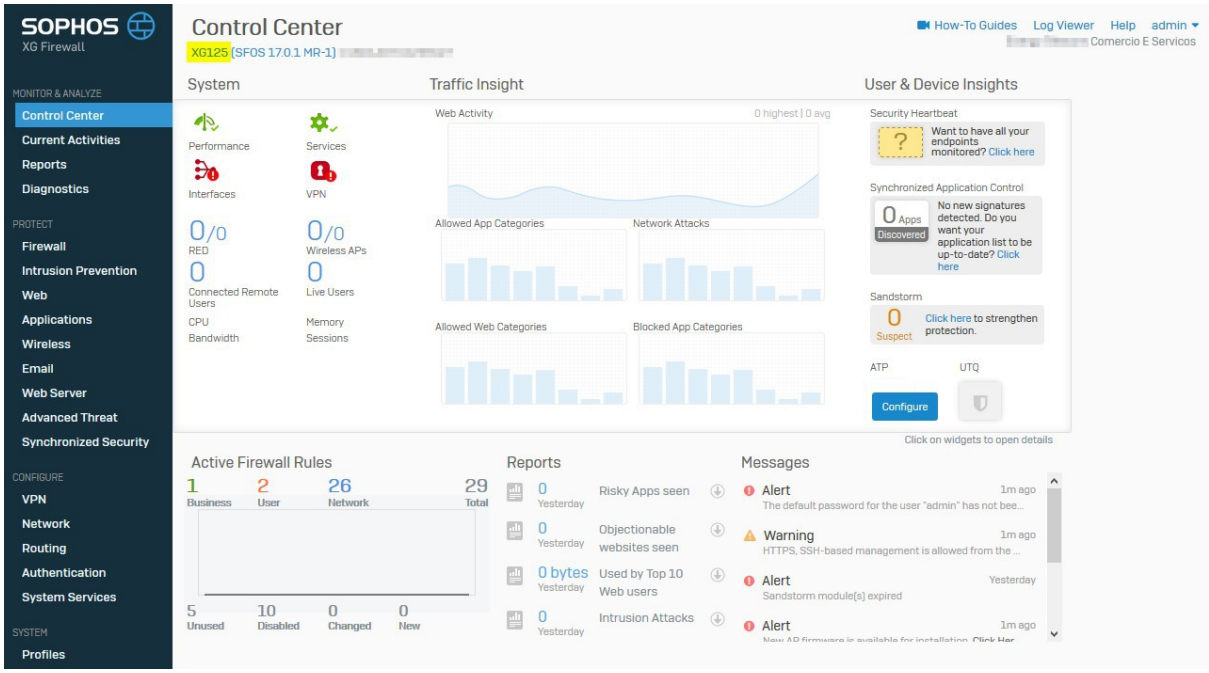
6.5.3 **Sophos**

A Sophos é uma empresa britânica desenvolvedora de *software* e *hardware* de segurança, incluindo antivírus, *anti-spyware*, *anti-spam*, controle de acesso de rede, *software* de criptografia e prevenção de perda de dados para desktops, servidores para proteção de sistemas de e-mail e filtragem para gateways da rede. A SophosLabs é a rede global de centros de análise de ameaças da empresa.

Recentemente a RC2 firmou uma parceria com a Sophos e tornou-se revendedora e prestadora de serviços credenciada no Brasil. Essa parceria possibilitou a implantação de dezenas de F*irewalls* XG, a nova linha de *firewalls* da empresa.

O Sophos XG *Firewall*, que possui mais detalhes técnicos no Anexo A, provê uma tecnologia altamente avançada, capaz de proteger redes de *ramsomwares* e ameaças avançadas com suas funcionalidades de IPS, proteção avançada contra ameaças, *sandboxing* em nuvem, dual antivírus, controle *web* e de aplicação, proteção de e-mail e um completo f*irewall* com alta performance e gerência otimizada.

Imagem 7 – *Dashboard* Sophos



Fonte: Elaborado pelo autor (2017)

6.6 Projeto de Segurança

O projeto de segurança está voltado aos mecanismos e ações de segurança a serem adotados, de forma que acessos não autorizados e vazamento de informações críticas ocorram no ambiente ou até mesmo fora dele.

O ponto primário é a garantia de acesso físico não autorizado. O NOC possui um rígido controle de acesso por biometria, onde somente a equipe técnica, gestão e diretoria são permitidos no ambiente. Assim, demais usuários da área comercial, marketing, estágio e afins, não terão qualquer tipo de contato com o ambiente de testes.

Além disso, foram elaboradas políticas de segurança com o objetivo de orientar usuários sobre seus direitos e deveres com relação a proteção das informações que são trafegadas, armazenadas e manipuladas no ambiente. O propósito das políticas de segurança é estabelecer diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

É de responsabilidade coletiva do NOC:

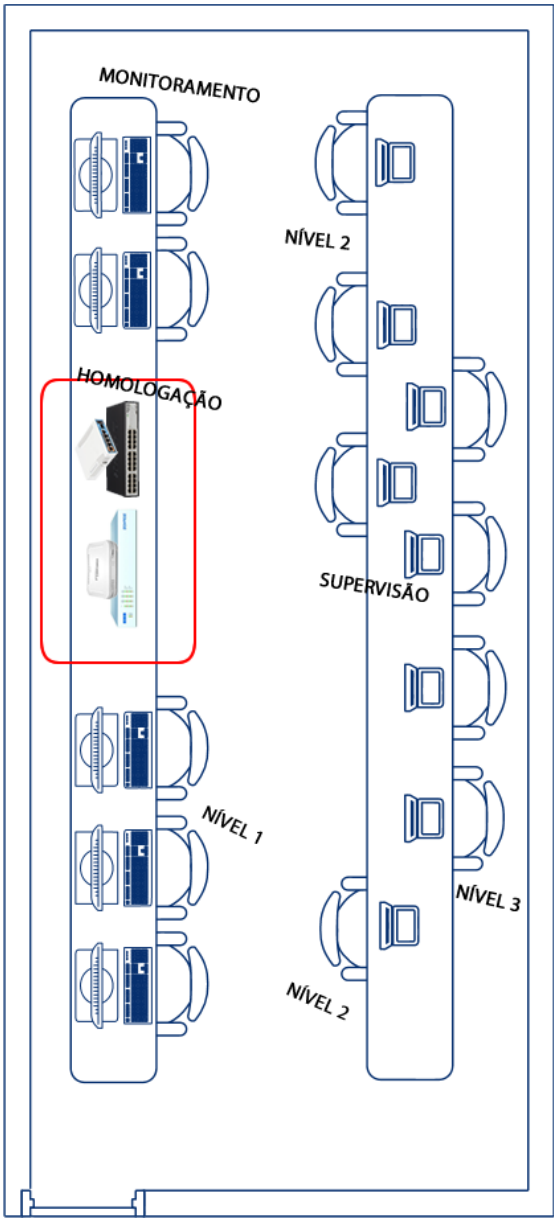
- Garantir a segurança física dos equipamentos, observando tentativas de violação ou adulteração.
- Garantir que vulnerabilidades e fragilidades dos equipamentos e aplicações sejam devidamente reportadas para a supervisão e gestão, e posteriormente ao fabricante.
- Propor investimentos, melhorias e alterações relacionadas ao funcionamento do ambiente de uma maneira geral
- Não compartilhar ou divulgar informações referente ao ambiente e atividades relacionadas a terceiros. Incidentes relacionados a esse usuário será de responsabilidade do próprio usuário.
- Zelar continuamente pela proteção das informações da entidade contra acesso, modificação, destruição e divulgação não autorizada.
- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas em prol da entidade.
- Não monitorar ou interceptar tráfego de dados do ambiente sem autorização.
- Não violar medidas de segurança ou de autenticação sem autorização.
- Comunicar a gestão e supervisão sobre qualquer anormalidade identificada na rede, sistema ou recursos que não tenha sido identificada pelo próprio núcleo.

7 PROJETO FÍSICO DA REDE

7.1 Centro de Operação de Rede (*Network Operations Center* – NOC)

A Figura 8 ilustra a distribuição dos equipamentos no ambiente de testes. O espaço do NOC é compartilhado pela equipe de monitoramento e analistas nível I, II e III, além da supervisão. O ambiente de testes está situado em uma área reservada para tal, com a devida organização dos equipamentos e cabeamento. A planta oficial não foi disponibilizada, então a proporção e distância entre os equipamentos são meramente ilustrativas.

Figura 8: NOC



Fonte: Elaborado pelo autor (2017)

7.2 Equipamentos de interconexão

A infraestrutura atual dispõe de todo o equipamento necessário para interconexão, dispensando a aquisição de novos equipamentos. A tabela a seguir lista esses equipamentos, com maiores detalhes de documentação no Anexo:

Tabela 7: Equipamentos de interconexão

Equipamento	Quantidade	Marca	Modelo	Localização
Servidor	1	DELL	Optiplex 7020	NOC
Switch 24 portas	1	D-Link	DES3028	NOC
Firewall	1	SonicWall	TZ 205	NOC
Firewall	1	Sophos	XG 125	NOC
Access Point	1	Aruba	IAP-103-RW	NOC
Roteador	1	Mikrotik	RB751U-2HnD	NOC

Fonte: Elaborado pelo autor (2017)

8 PLANO DE IMPLANTAÇÃO

8.1 Cronograma

A Tabela 8 descreve o cronograma de implantação do projeto, tendo iniciadas as atividades no dia 16 de Outubro.

Tabela 8: Cronograma

Data de término	Ponto de controle
16 Outubro	Instalação e configuração servidor Windows Server
17 Outubro	Instalação e configuração PRTG e máquinas virtuais no servidor
18 Outubro	Instalação e configuração Mikrotik e Switch, testes de conectividade
19 Outubro	Instalação e configuração SonicWall e Sophos, testes de conectividade
20 Outubro	Instalação Aruba e interligação dos equipamentos Normatização das políticas de segurança
23 Outubro	Configurações e testes finais Relatório dos testes, documentação, entrega do ambiente
Contínuo	Acompanhamento

Fonte: Elaborado pelo autor (2017)

8.2 Plano de entrega

O plano de entrega do projeto é um ponto simples, porém importante para que os usuários saibam o que é e como acessar o ambiente disponibilizado. Para isso, foi formalizado via e-mail para o grupo do suporte, onde todos devem obrigatoriamente ler as informações recebidas, todas as informações pertinentes para acesso do ambiente. Entre elas: endereços IP para acesso aos equipamentos, credenciais de acesso, documentação dos equipamentos, políticas de segurança e direitos e deveres que serão detalhados na seção 8.3.

8.3 Plano de avaliação

Uma vez implantado e entregue o projeto, é necessário um plano de acompanhamento e avaliação para que as atividades realizadas estejam cumprindo os requisitos definidos. Esse plano foi dividido em 4 categorias: disponibilidade, desempenho, documentação e usabilidade.

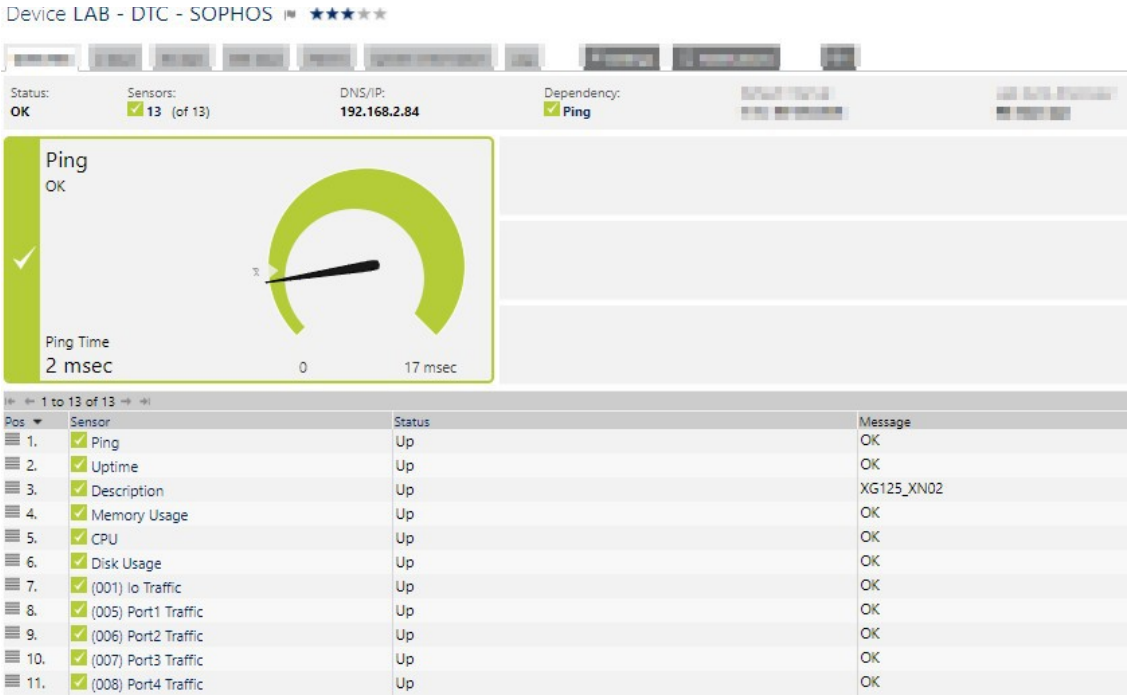
8.3.1 Disponibilidade

É importante ressaltar que a disponibilidade não é uma prioridade nos objetivos técnicos, porém essa disponibilidade está relacionada a atividades programadas. Ou seja, o ambiente estará indisponível apenas se houver um agendamento para tal. Falhas inesperadas precisam ser detectadas e devidamente tratadas para que o ambiente esteja operando dentro das condições normais. Por isso, foi adicionado ao servidor PRTG de produção o monitoramento dos *firewalls* SonicWall e Sophos, conforme ilustrado nas Figuras 9 e 10:

Figura 9: Monitoramento SonicWall

Fonte: Elaborado pelo autor (2017)

Figura 10: Monitoramento Sophos



Fonte: Elaborado pelo autor (2017)

Através desse monitoramento, será possível identificar eventos que ocorrem mesmo fora de uma janela de atividade programada. Alto processamento, estouro de memória, falhas no cabeamento e indisponibilidade da gerência via web são exemplos de eventos que podem ser identificados e então tratados.

8.3.2 Desempenho

Foi definido que o ambiente não terá limitações de banda para os equipamentos. Dessa forma, o link de 1Gbps redundante utilizado pelo NOC será compartilhado com o ambiente de testes sem restrições, possibilitando que atualizações e demais atividades que necessitem de uma conexão estável sejam executadas de forma ágil e sem interrupções.

8.3.3 Documentação

Documentar as atividades realizadas no ambiente é importante não só para uma base de conhecimento pessoal, mas também para que toda a equipe tenha acessibilidade às informações e configurações que possam ser relevantes. Por isso, qualquer atividade realizada no ambiente será formalizada via e-mail, para a equipe de suporte. As descrições precisam ser claras e objetivas, como a necessidade de tal atividade e os resultados obtidos. Problemas enfrentados também podem ser apresentados, o que permitirá a ajuda mútua para buscar a solução.

8.3.4 Usabilidade

Utilizando a documentação como base, é importante que o ambiente ofereça ao usuário uma usabilidade adequada. Cabeamento sem um padrão e identificação precisa ser evitado e será acompanhado constantemente. Além disso, cada usuário terá um backup individual das configurações dos equipamentos. Essa prática foi definida para evitar que um usuário tenha acesso a um ambiente que possua configurações aplicadas para um determinado propósito e elas sejam modificadas. Portanto, ao término de qualquer atividade, um backup das configurações deverá ser exportado, ou o usuário correrá o risco de perde-las em um próximo acesso.

9 CONCLUSÃO

Esse projeto apresentou uma solução capaz de auxiliar no aprimoramento teórico e técnico dos funcionários da RC2, sem a necessidade de um treinamento oficial custeado pela empresa, ao mesmo tempo que esse aprendizado seja isolado do ambiente de produção, sem possíveis impactos aos clientes.

Com a implantação do projeto e a execução das atividades no ambiente de testes seguindo o escopo definido, muitos benefícios e resultados positivos foram obtidos. Atividades e simulações para ambientes complexos foram possíveis, além de informações e lições aprendidas. Alguns dos resultados mais importantes são:

- Criação de *templates* personalizados no PRTG para equipamentos SonicWall, Sophos e Checkpoint, além de servidores Windows e Linux;
- Integração de *firewalls* com o *Active Directory*, utilizando autenticação transparente;
- Homologação de novas firmwares dos equipamentos;
- Configuração de VPN entre SonicWall x Sophos x Mikrotik;
- Teste de *failover* de rotas VPN e MPLS;
- Implementação de autenticação via SSO com Radius integrado ao *Active Directory* utilizando Aruba;
- Instalação de certificado digital do Sophos para inspeção e bloqueio de tráfego SSL de aplicações e conteúdo *web*;
- Inspeção e bloqueio de e-mails baseado no título e extensões dos anexos;
- Testes de liberação e bloqueio de conteúdo baseados em *schedules*.

Esses resultados reforçaram e justificaram a necessidade da implantação do ambiente de testes. Além disso, *feedbacks* positivos por parte dos clientes através das soluções atendidas com sucesso valorizaram não só a imagem da empresa, mas também o profissional envolvido nas resoluções, motivando-o cada vez mais para seu crescimento.

Um ambiente mais colaborativo também foi estimulado através desse projeto, uma vez que nas dificuldades encontradas para algumas soluções, o compartilhamento de conhecimento foi fundamental para o sucesso delas. Essas interações também permitiram sugestões para melhorias do ambiente que já estão em fase de planejamento -respeitando a escalabilidade do ambiente-, como implantação de outros modelos de *firewalls* SonicWall e Sophos e também equipamentos de outros fabricantes, como Checkpoint e MAfee *Webgateway*. Melhorias essas que serão sempre aplicadas na medida do possível para que o sucesso individual e coletivo seja alcançado.

REFERÊNCIAS

PINHEIRO, J. M. S. **Gerenciamento de Redes de Computadores: Uma Breve Introdução**. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acesso em: 25 out. 2017.

CHERDANTSEVA, Y.; HILTON, J. **A Reference Model of Information Assurance & Security**. In: IEEE proceedings of ARES 2013. Germany: IEEE, 2013. p. 1.

CLEMM, A. **Network Management Fundamentals**. Indianapolis: Cisco Press, 2007. 532p.

BRAUMANN, R.; CAVIN, S.; SCHMID, S. **Voice Over IP – Security and SPIT**. Disponível em: http://scholar.googleusercontent.com/scholar?q=cache:uYD9e_DMEZsJ:scholar.google.com/+VoIP+Security+Threats&hl=pt-BR&as_sdt=0. Acesso em: 3 fev. 2017.

FILHO, O. P. **Gerenciamento e Monitoramento de Rede II: Gerenciamento SNMP**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes2/pagina_2.asp>. Acesso em: 3 fev. 2017.

PORTELLA, A. Y.; MONTEIRO, J. C. E.; MOREIRA, V. A. B. **Segurança em smart grid**. Disponível em: <http://www.gta.ufrj.br/grad/12_1/seg_smartgrid/index.html>. Acesso em: 3 fev. 2017.

FEARN, N. **Top 5 best network monitoring tools and software of 2017**. Disponível em: <http://www.techradar.com/news/top-5-best-network-monitoring-tools-of-2017>. Acesso em: 05 nov. 2017.

SONICWALL. **Relatório Anual de Ameaças, 2017.** Disponível em: <https://www.gruppen.com.br/sonicwall/assets/download/2017-sonic-wall--threat-report--visual-summary-pt.pdf>. Acesso em: 12 nov. 2017.

ANEXO A – ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS

Desktop Dell OptiPlex 7020 SFF i5-4590 | 4GB | 500GB

Tipo	**Desktop**
Processador	**Intel® Core™i5-4590 Quad Core**
Frequência	**3,3 GHz**
Turbo Boost / Burst	**3,7 GHz**
Cache Processador	**6 MB**
Memória RAM	**4 GB**
Tipo Memória	**DDR3-1600**
Disco Rígido	**500 GB (7200 RPM)**
Placa Gráfica	**Intel® HD Graphics 4600**
Sistema Áudio	**Áudio HD**
Drive Ótica	**Leitor DVD±RW**
Comunicações	**Rede Gigabit 10/100/1000**
Interfaces	**4x USB 3.0**
	6x USB 2.0
	1x VGA
	3x Jack 3,5mm
Monitor	**Não**
Sistema Operativo	**Windows 7 Pro**
Dimensões	**29 x 9,3 x 31,2 cm**
Peso	**6 kg**

Switch de Rede D-Link DES 3028

Interface

Number of 10/100BASE-TX ports
DES-3028P - 24 ports

DES-3052P - 48 ports

Number of 10/100/1000BASE-T ports
2

Number of Combo 1000Base-T/SFP ports
2

PoE Supported Models (Standard(s)/Number of Ports/Maximum Power Budget)
DES-3028P (802.3af/24 ports/185W)

DES-3052P (802.3af/48 ports/370W)

RS-232 Console Port
Yes

Performance

Switch Capacity
DES-3028P - 12.8 Gbps

DES-3052P - 17.6 Gbps

64-Byte Packet Forwarding Rate
DES-3028P - 9.5 Mpps

DES-3052P - 13.1 Mpps

MAC Address Table Size
8K

Packet Buffer
512KB

Flash Memory
8MB

Jumbo Frame
2048 Bytes (tagged)

2044 Bytes (untagged)

Diagnostic LED Indicators
Power (Per Device)
Yes

Console (Per Device)
Yes
Link/Activity (Per Port)
Yes
Speed Indicator (Per Port)
Yes

Physical & Environmental

Power Consumption
DES-3028P - 217W
DES-3052P - 395W
Power Input
100 to 240 VAC, 50 to 60HZ Internal Universal Power Supply
Dimensions (W x D x H)
DES-3028P - 441mm x 207mm x 44mm (17.36 x 8.15 x 1.73 inches)
DES-3052P - 441mm x 309mm x 44mm (17.36 x 12.17 x 1.73 inches)
Size
19-inch Standard Rack-Mount Width, 1U Height
Ventilation
DES-3028P - 2 DC fans
DES-3052P - 3 DC fans
Heat Dissipation
DES-3028P - 742.7 BTU per hour
DES-3052P - 1347 BTU per hour
MTBF
DES-3028P - 196,033 hours
DES-3052P - 169,182 hours
Temperature
Operating: 0° to 40°C (32° to 104°F)
Storage: -40° to 70°C (-40° to 158°F)
Operating Humidity
5% ~ 95% Non-condensing
EMI/EMC
FCC Class A, CE, C-Tick, VCCI Class A
Safety
cUL, LVD

Software Feature

Stackability
Virtual Stacking:
Supports D-Link Single IP Management
Up to 32 devices per Virtual Stack
L2 Features
MAC Address Table: 8k
Jumbo Frames support up to 2048 bytes
IGMP Snooping:
IGMP v1/v2 Snooping
Supports 256 groups
Port-based IGMP Snooping Fast Leave
Limited IP Multicasting:

Up to 24 IGMP filtering profiles, 128 ranges per profile
MLD Snooping:

MLD v1/v2 Snooping
Supports 256 groups
MLD Snooping Fast Leave
IGMP Authentication
Spanning Tree:
802.1D-2004 Edition STP
802.1w RSTP
802.1s MSTP
BPDU Filtering
Root Restriction
Loopback Detection (LBD)
802.3ad Link Aggregation:
Max. 6 groups per device, 8 ports per group
Port Mirroring:
Supports One-to-One, Many-to-One, Flow-based Mirroring
Flow Control:
802.3x Flow Control
HoL Blocking Prevention

VLAN

802.1Q Tagged VLAN
VLAN Group:
Max. 4K VLAN
Port-based VLAN
GVRP:
Max. 255 Dynamic VLAN
Asymmetric VLAN
Double VLAN (Q-in-Q):
Port-based Q-in-Q
ISM VLAN

Quality of Service (QoS)

Bandwidth Control:
Port-based (Ingress/Egress, min. granularity
64kbps) Flow-based (Ingress, min. granularity
64kbps)
4 queues per port
802.1p Quality of Service
Queue Handling:
Strict
Weighted Round Robin (WRR)
CoS based on:
Switch Port
VLAN ID
802.1p Priority Queues
MAC Address

IP Address
DSCP
Protocol Type
TCP/UDP Port
User-Defined Packet Content
Time Based QoS

Access Control List (ACL)
Up to 256 Access Rules
ACL based on:
802.1p Priority
VLAN ID
MAC Address
Ether Type
IP Address
DSCP
Protocol Type
TCP/UDP Port Number
User Defined Packet Content
Time-based ACL
CPU Interface Filtering

Roteador de Borda Mikrotik RB751U-2HnD

Details
Product code RB751U-2HnD
Architecture MIPSBE
CPU AR7241
CPU core count 1
CPU nominal frequency 400 MHz
Dimensions 113x138x29mm
License level 4
Operating System RouterOS
Size of RAM 32 MB
Storage size 64 MB
Storage type NAND
Tested ambient temperature -20C .. +50C
Suggested price $59.95
Powering

Details
Max Power consumption 10W
PoE in Passive PoE

Number of DC inputs 1
Wireless

Details
Wireless 2.4 GHz number of chains 2
Wireless 2.4 GHz standards 802.11b/g/n
Antenna gain dBi for 2.4 GHz 2.5
Wireless 2.4 GHz chip model AR9283
Ethernet

Details
10/100 Ethernet ports 5
Peripherals

Details
Number of USB ports1

Firewall SonicWall TZ 205

TZ 205 Series	
Firewall	
SonicOS Version	SonicOS 5.8.1 and later
Stateful Throughput1	500 Mbps
IPS Throughput2	80 Mbps
GAV Throughput2	60 Mbps
UTM Throughput2	40 Mbps
Maximum Connections3	12
Maximum UTM/DPI Connections	12
New Connections/Sec	1,5
Nodes Supported	Unrestricted

Denial of Service Attack Protection	22 classes of DoS, DDoS and scanning attacks
SonicPoints Supported	2
VPN	**TZ 205 Series**
3DES/AES Throughput[4]	100 Mbps
Site-to-Site VPN Tunnels	10
Bundled Global VPN Client Licenses (maximum)	2 (10)
Bundled SSL VPN Licenses (maximum)	1 (10)
Encryption/Authentication/DH Group	DES, 3DES, AES (128, 142, 256-bit), MD5, SHA-1, SHA-2/DH Group 1, 2, 5, 14
Virtual Assist Bundled (Maximum)	30-day trial (1)
Key Exchange	IKE, Manual Key, Certificates (X.509), L2TP over IPSec
Certificate Support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWALL-to-SonicWALL VPN, SCEP
VPN Features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN
Global VPN Client Platforms Supported	Microsoft® Windows XP, Vista 32/64-bit, Windows 7 32/64-bit
SSL VPN Platforms Supported	Microsoft Windows XP/Vista 32/64-bit/Windows 7, Mac OSX 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE
Mobile Connect Platform	Apple® iOS 4.2 or higher, Google® Android™ 4.0 or higher

Security Services	TZ 205 Series
Deep Packet Inspection Services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control (TZ 215 only)
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, ActiveX, Java Applet, and cookie blocking bandwidth management on filtering categories, allow/forbid lists
Enforced Client Anti-Virus and Anti-Spyware	McAfee®
Comprehensive Anti-Spam Service[6]	Supported
Application Intelligence and Control	Application Control
Networking	**TZ 205 Series**
IP Address Assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay
NAT Modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode
VLANs	10, Portshield
DHCP	Internal server, relay
Routing	OSPF, RIP v1/v2, static routes, policy-based routing, multicast
Authentication	LDAP, Local DB, RADIUS, XAUTH, X-Forwarders[8]
Single sign-on	AD, eDirectory, RADIUS Accounting, NTLM, X-Forwarders[8]
Local User Database	150 users

VoIP	Full H.323v1-5, SIP, gatekeeper support, outbound bandwidth management, VoIP over WLAN,deep inspection security, full interoperability with most VoIP gateway and communications devices
System	**TZ 205 Series**
Zone Security	Yes
Schedules	Yes
Object-based/Group-based Management	Yes
DDNS	Dynamic DNS providers include: dyndns.org, yi.org, no-ip.com and changeip.com
Management and Monitoring	Local CLI, Web GUI (HTTP, HTTPS), SNMP v3; Global management with SonicWALL GMS
Logging and Reporting	Analyzer, Scrutinizer, GMS, Local Log, Syslog, Solera Networks, NetFlow v5/v9 (TZ 215), IPFIX with Extensions (TZ 215), Real-time Visualization (TZ 215 only)
Hardware Failover	Active/Passive
Anti-Spam	RBL support, Allowed/Blocked Lists, Optional SonicWALL Comprehensive Anti-Spam Service[6]
Load Balancing	Yes, Outgoing and Incoming
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3
WAN Acceleration Support[7]	Yes, with SonicWALL WXA appliances
Built-in Wireless LAN	**TZ 205W Series**
Standards	802.11a/b/g/n (3x3)

Wireless Security Standards	WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS
Virtual Access Points (VAPs)	Up to 8
Antennas	Triple: 2 external detachable, 1 internal
Radio Power: 802.11b/802.11g/802.11n	15.5 dBm max/18 dBm max/17 dBM @ 6 Mbps, 13 dBM @ 54 Mbps
Radio Power: 802.11a/802.11b/802.11g/802.11n	15.5 dBm max/18 dBm max/17 dBM @ 6 Mbps, 13 dBM @ 54 Mbps
Radio Power: 802.11n (2.4GHz)/802.11n (5.0GHz)	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15
Radio Receive Sensitivity: **802.11a/802.11b/802.11g**	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm @ 11Mbps/-91 dBm @ 6Mbps, -74 dBm @ 54 Mbps
Radio Receive Sensitivity: **802.11n (2.4GHz)/802.11n (5.0GHz)**	-89 dBm MCS 0, -70 dBm MCS 15/-95 dBm MCS 0, -76 dBm MCS 15
Hardware	**TZ 205 Series**
Interfaces	(5) 10/100/1000 Copper Gigabit, 1 USB, 1 Console
Processor	Dual-Core
Flash Memory/RAM	32 MB/256 MB

3G Wireless/Modem[5]	Supported with approved adapters[5]
USB Ports	1
Power Input	100 to 240 VAC, 50-60 Hz, 1 A
Max Power Consumption	6.4W/10.5W
Total Heat Dissipation	21.9 BTU/35.8 BTU
Certifications	VPNC, ICSA Firewall 4.1
Certifications Pending	EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2
Dimensions	5.555 x 1.42 x 7.48 in (14.1 x 3.6 x 19 cm)
Weight	0.75 lbs/0.34 kg 0.84 lbs/0.38 kg
Major Regulatory Compliance	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, NOM, UL, cUL, TUV/GS, CB, NOM, WEEE, RoHS
Environment/Humidity	40-105° F, 0-40° C/ 5-95% non-condensing
MTB	28 years/15 years

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.
[3] Actual maximum connection counts are lower when DPI services are enabled.
[4] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.
[5] 3G card and modem are not included. See http://www.sonicwall.com/us/products/cardsupport.html for supported USB devices.
[6] The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less.
[7] With SonicWALL WXA Series Appliances.
[8] Web proxy using X-Forwarded-For

Firewall Sophos XG 125

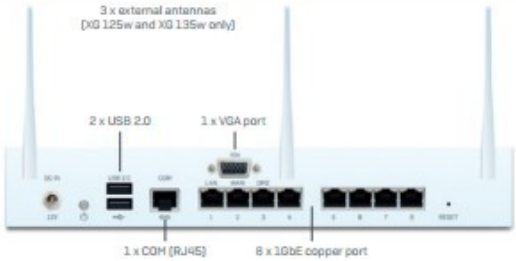
Sophos XG Series Desktop Appliances: XG 125, XG 125w, XG 135, XG 135w

Technical Specifications

These powerful firewall appliances offer 1U performance with a desktop form factor and price. If you have a small business or branch offices to protect and are working on a tight budget, these models are the ideal choice. They are also available with integrated 802.11ac wireless LAN for optimal coverage and connectivity for your mobile workers. Built upon the latest Intel architecture, our software makes optimal use of the multi-core technology to provide excellent throughput for all your key processes. These models come equipped with 8 GbE copper ports built-in.

Front View

Back View



Environment	
Power consumption	12.46W, 49.3 BTU/hr (idle) 26.16W, 89.2 BTU/hr (full load)
Operating temperature	0-40°C (operating) -20 to +80°C (storage)
Humidity	10%-90%, non-condensing

Product Certifications	
Certifications	CB, CE, FCC Class B, IC, VCCI, MIC, RCM, UL, CCC

Performance[1]	XG 125(w) Rev. 2	XG 135(w) Rev. 2
Firewall throughput	5 Gbps	7 Gbps
Firewall IMIX	1.75 Gbps	2.75 Gbps
VPN throughput	410 Mbps	950 Mbps
IPS throughput	1 Gbps	1.75 Gbps
NGFW (IPS + App Ctrl + WebFilter) max.	360 Mbps	880 Mbps
Antivirus throughput (proxy)	590 Mbps	1.4 Gbps
Concurrent connections	6,200,000	8,200,000
New connections/sec	35,000	82,000
Maximum licensed users	unrestricted	unrestricted

Wireless Specification (XG 125w and XG 135w only)	
No. of antennas	3 external
MIMO capabilities	3 x 3:3
Wireless interface	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)

Physical interfaces	
Storage (local quarantine/logs)	integrated SSD
Ethernet interfaces (fixed)	8 GE copper
I/O ports (rear)	2 x USB 2.0 1 x COM (RJ45) 1 x VGA
Power supply	External auto ranging DC: 12V, 100-240VAC, 50-60 Hz

Physical specifications	
Mounting	Rackmount kit available (to be ordered separately)
Dimensions Width x Depth x Height	288 x 186.8 x 44 mm 11.38 x 7.35 x 1.73 inches
Weight	1.7 kg / 3.75 lbs (unpacked) 2.82 kg / 6.22 lbs (packed)

Access Point Aruba IAP-103-RW

GENERAL	
Power Over Ethernet (PoE)	PoE+
Manufacturer	Aruba Networks, Inc.
MODEM	
Antenna Qty	4
POWER DEVICE	
Nominal Voltage	DC 48 V
INTERFACE PROVIDED	
Qty	1
NETWORKING	
Data Transfer Rate	300 Mbps
Line Coding Format	BPSK
Status Indicators	power
Spread Spectrum	Method OFDM
Features	Trusted Platform Module (TPM)
Data Link Protocol	IEEE 802.11b
Compliant Standards	IEEE 802.11a
Connectivity Technology	wireless
ANTENNA	
Directivity	omni-directional
ENVIRONMENTAL PARAMETERS	
Min Operating Temperature	32 °F
Max Operating Temperature	104 °F

HEADER	
Brand	Aruba
Product Line	Aruba Instant
Model	IAP-103
Country Kits	Rest of World
Packaged Quantity	1
Compatibility	PC
SERVICE & SUPPORT	
Type	limited lifetime warranty
DIMENSIONS & WEIGHT	
Width	5.9 in
Depth	5.9 in
Height	1.6 in
Weight	10.6 oz
SERVICE & SUPPORT DETAILS	
Full Contract Period	lifetime
GENERAL	
Manufacturer	Aruba Networks, Inc.