PRODAM

Processamento de Dados Amazonas S. A.
Governo do Amazonas

PRODAM 40ANOS
TECNOLOGIA EM SUA VIDA

Check-list realizado no Teste de Aderência previsto no Anexo IV – Pregão Eletrônico 12/2012

Licitante: Energy Telecom **Data: 09/01/2012**

Participantes da PRODAM:

Regis Muller
Alexandre Franciscani Ferreira
Gustavo Simonetti Bomfim

Participante da LICITANTE:

Emanoel Carneiro

Equipamento testado:

Firewall Sonicwall modelo TZ-215 wireless

Rua Jonathas Pedrosa, 1937 – Praça 14 – Manaus – AM CEP 69020-110 Telefone (92) 2121-6500 Fax (92) 3232-4369
E-mail: prodam@prodam.am.gov.br Site: http://prodam.am.gov.br

ANEXO IV

TESTES DE ADERÊNCIA

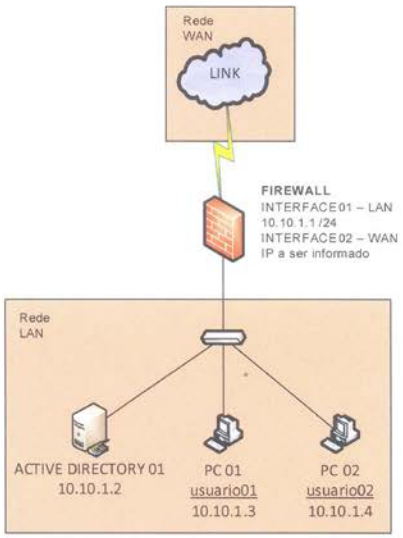

Figura 1 – Teste de aderência para *Firewall UTM*.

1. Arquitetura do Ambiente

A Figura 1 apresenta o ambiente de rede nas dependências da CONTRATANTE para o qual a LICITANTE classificada como vencedora deverá configurar o seu Appliance de firewall UTM afim de possibilitar o Teste de Aderência.

A arquitetura do ambiente é composta por 02 (dois) seguimentos de rede:
1) Rede *LAN*;
2) Rede *WAN*;

A Rede *LAN* possui 02 (dois) computadores (PC 01 e PC 02) e hospeda o Servidor Controlador de Domínio (*Active Directory* 01), que é o responsável pela autenticação dos usuários na rede interna; e a Rede *WAN* possui um link de acesso para a Internet.

As responsabilidades pelo fornecimento dos equipamentos estão descritas na tabela 4:

Equipamento	Fornecimento
Firewall	LICITANTE
Switch	CONTRATANTE
PC 01, PC 02	CONTRATANTE
Cabos de rede e pontos elétricos	CONTRATANTE
Link de Internet	CONTRATANTE
Servidor de *Active Directory*	CONTRATANTE

Tabela 4 – Tabela de responsabilidade pelo fornecimento dos equipamentos para testes.

2. Configurações necessárias ao ambiente:

Equipamento	Configurações
Firewall	1) *Configurar a geração de relatórios* (teste 3.1.1); 2) Ativar e testar o serviço de *DHCP (teste 3.1.2);* 3) Efetuar controle *Web* com autenticação no *AD* sem instalação de *software* na máquina e alteração das configurações no browser (teste 3.1.3); 4) Aplicar regra por usuário e por horário (teste 3.1.4); 5) Controlar os acessos *web* por categorias de *sites*, com base diariamente atualizada, e atribuir perfil por endereço IP (teste 3.1.5); 6) Detectar e bloquear aplicativos em tempo real (teste 3.1.6); 7) Atualizar automaticamente as assinaturas de vírus, spyware e *IPS* (teste 3.1.7); 8) Ativar e testar o IPS (teste 3.1.8); 9) Ativar e testar as regras de antivirus e antispyware (teste 3.1.9); 10) Ativar e testar o recurso de inspeção HTTPS/SSL para o filtro de conteúdo web, antivírus e antispyware (teste 3.1.10); 11) Limitar o número máximo de conexões simultâneas, aplicando individualmenté para cada regra de filtragem (teste 3.1.11); 12) Aplicar controle de banda por usuário (teste 3.1.12); 13) Aplicar QoS por protocolo (teste 3.1.13); 14) Apresentar relatórios sobre os acessos efetuados neste teste de aderência (teste 3.1.14).
PC 01 e 02	1) Servir para a realização dos testes de acesso.
Link de Internet	1) Permitir os testes com acessos à Internet (testes 3.1.1, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 3.1.9, 3.1.10, 3.1.11, 3.1.12 e 3.1.13).
Servidor *Active Directory*	1) Autenticar os usuários da rede *LAN*.

Tabela 5 – Comportamento esperado pelo ambiente

3. Roteiro dos testes:

3.1. Solução em *Appliance* de *Firewall UTM*:

Configuração a ser testada	Testes	Aceito (S/N)
3.1.1 Configurar *a geração de relatórios* para apresentação sob os testes a serem realizados;	1. Configurar a geração dos seguintes relatórios, no horário de 8h00 às 18h00, em servidor externo a Prodam: - Acessos web por categoria; - Acessos por aplicação; - Vírus e Spywares; - IPS.	OK
3.1.2 Ativar e testar o serviço de *DHCP*;	1. Ativar o serviço de *DHCP* no *Firewall*, atribuir e testar os seguintes endereços *IPs*: 2. 10.10.1.3 /24 para o PC 01, com Gateway 10.10.1.1 e DNS 200.242.43.142; 3. 10.10.1.4 /24 para o PC 02, com Gateway 10.10.1.1 e DNS 200.242.43.142; 4. Apresentar a entrega dos *IPs* aos computadores.	OK
3.1.3 Permitir o controle de	1. Configurar o *Firewall* para integrar-se ao *Active Directory*	

	acesso por usuário, através da autenticação utilizando servidor *Active Directory*, de forma automática, sem a instalação de *softwares* adicionais nas estações de trabalho e sem configuração adicional no browser;	de forma que consiga visualizar os usuários "usuario01" e "usuario02"; 2. Instalar e configurar o software de autenticação automática no Active Directory; 3. Liberar o acesso *HTTP* para o usuário01 e bloquear para o usuario02; 4. Liberar o acesso do aplicativo *Skype* para o usuario02 e bloquear para o usuário01; 5. Efetuar os acessos na Internet *HTTP* e do aplicativo *Skype* com os dois usuários autenticados no domínio, sem que seja necessário a instalação de softwares adicionais nas estações e se autenticar no browser ou alterar suas configurações; 6. Apresentar as liberações e bloqueios efetuados pelo *firewall*.	OK
3.1.4	Aplicar regra de *firewall* por usuário e por horário;	1. Configurar a liberação *HTTP* apenas para o usuario01, para os próximos 10 minutos a partir da criação da regra; 2. Verificar se o usuário "usuario01" acessa com sucesso a internet via *HTTP* e se o usuário "usuario02" está bloqueado; 3. Verificar se, passados 10 minutos, o acesso *HTTP* do usuario01 é bloqueado.	OK
3.1.5	Controlar o conteúdo *web* por categorias de *sites*, com base de dados diariamente atualizada pelo fabricante, e permitir a atribuição de perfil por faixa de endereço IP;	1. Criar o perfil "funcionários" no *Firewall* liberando apenas as categorias de *sites web* "Portais" e "Redes Sociais", ou categoria equivalente de *sites* relacionados a portais e redes sociais; 2. Vincular o perfil de acesso "funcionários" ao range de IP 10.10.1.3 ao 10.10.1.254; 3. Atualizar a base de assinaturas das categorias de *sites*; 4. Apresentar que a atualização foi efetuada, ou caso já esteja atualizada, apresentar que houve a consulta na base de assinaturas e a última versão já está presente no *firewall*; 5. A partir do PC01 e PC02 acessar os *sites* http://www.uol.com.br, http://www.terra.com.br, http://www.facebook.com e http://www.orkut.com 6. Apresentar as liberações de acessos efetuadas pelo *firewall*.	OK
3.1.6	Detectar e bloquear em tempo real aplicativos *P2P* (*peer-to-peer*), MSN (nova versão do *Windows Live* da *Microsoft*) e o *Skype* para usuários da rede;	1. Configurar o bloqueio de *P2P*, *Windows Live Messenger* em sua nova versão e *Skype* apenas para o usuário01; 2. Testar o acesso aos 3 aplicativos, a partir do PC 01 e PC 02, e aferir que estão bloqueados para o usuário01 logado no PC 01 e liberados para o usuário02 no PC 02.	OK
3.1.7	Atualizar automaticamente as assinaturas de vírus, spyware e *IPS* sem a necessidade de intervenção humana;	1. Configurar a atualização automática no *Firewall*; 2. Apresentar que a atualização foi efetuada, ou caso já esteja atualizada, apresentar que houve a consulta na base de assinaturas e a última versão já está presente no *firewall*.	OK
3.1.8	Ativar e testar o recurso de IPS;	1. Ativar no Firewall o recurso de IPS; 2. Realizar o acesso externo, com o PC01, a um servidor próprio da LICITANTE simulando testes de ataques; 3. Apresentar a análise efetuada pelo *firewall* com o recurso	OK

		de IPS.	
3.1.9	Ativar e testar os recursos de antivírus e antispyware;	4. Ativar no Firewall os recursos de antivírus e antispyware; 5. Realizar o *download*, com o PC01 e 02, do arquivo hospedado no endereço: ftp://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz 6. Apresentar a análise efetuada pelo *firewall* com os recursos de antivírus e antispyware.	OK
3.1.10	Ativar e testar o recurso de inspeção HTTPS/SSL para o filtro de conteúdo web, antivírus e antispyware;	1. Ativar no Firewall os recursos de inspeção HTTPS/SSL para o filtro de conteúdo web, antivírus e antispyware, *de modo que o filtro de conteúdo previna o acesso às redes sociais via HTTPS e o antivírus e antispyware previnam o download de arquivos infectados*; 2. Acessar, com o PC01 e 02, os *sites*: https://www.orkut.com.br e https://secure.eicar.org/eicarcom 3. Apresentar a detecção e bloqueio da análise SSL sob os recursos de filtro de conteúdo, antivírus e antispyware.	OK
3.1.11	Limitar o número máximo de conexões simultâneas, aplicando individualmente para cada regra de filtragem;	1. Configurar a regra de *firewall* que libera o acesso *HTTP* para o website http://www.terra.com.br com limite máximo de 2 conexões, e para o website http://www.uol.com.br com o limite de conexões padrão do *firewall*; 2. Testar o acesso *HTTP*, com o PC 01, ao website http://www.terra.com.br; 3. Apresentar que o acesso chegou ao limite de conexões estabelecido pelo *firewall*; 4. Testar o acesso *HTTP*, com o PC 01, ao *site* http://www.uol.com.br 5. Apresentar que o acesso não chegou ao limite de conexões estabelecido pelo *firewall*.	OK
3.1.12	Aplicar controle de banda por usuário;	1. Configurar o *Firewall* para controlar a banda do "usuario01" em 64Kbps para saídas com o protocolo *HTTP* e 512Kbps para saídas com o protocolo *FTP*, além de controlar a banda do "usuario02" em 512Kbps para saídas com o protocolo *HTTP* e sem controle de banda para saídas com o protocolo *FTP*; 2. A partir do "usuario01" logado no PC01, efetuar o seguinte *download* na Internet através de: 3. *HTTP*: http://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz 4. *FTP*: ftp://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz 5. A partir do "usuario02" logado no PC02, efetuar o seguinte *download* na Internet através de: 6. *HTTP*: http://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz 7. *FTP*: ftp://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz 8. Apresentar o controle de banda efetuado pelo *firewall* com os usuários "usuario01" e "usuario02", nos protocolos *HTTP* e *FTP*.	OK
3.1.13	Aplicar QoS por protocolo;	1. Configurar o *Firewall* para priorizar requisições *HTTP*, comparadas às requisições *FTP*; 2. A partir do PC01, efetuar o seguinte *download* na Internet através de: 3. *HTTP*: http://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz 4. *FTP*: ftp://ftp.br.debian.org/debian-backports/pool/main/a/altos/altos_1.0.3~bpo60+1.tar.gz	OK

	5. Apresentar a priorização efetuada pelo *firewall* no protocolo *HTTP*, comparada ao *FTP*.	
3.1.14 Apresentar relatórios sobre os acessos efetuados.	1. Apresentar os seguintes relatórios no horário de 8h00 às 18h00: - Acessos web por categoria (testado no item 3.1.5); - Acessos por aplicação (testado no item 3.1.6); - IPS (testado no item 3.1.8); - Vírus e Spywares (testado no item 3.1.10).	OK

Tabela 6: Roteiro dos testes para a solução em *Appliance* de *Firewall UTM*.

Resultado dos testes de aderência: APROVADO

Manaus, 09 de janeiro de 2013.

Regis Alberto Müller da Silva
Assessor Técnico

Alexandre Franciscani Ferreira
Supervisor de Segurança da Informação