TEST REPORT
Tolly.

#212148
Novembro de 2012

Encomendada pela
IBM Security Systems Division

Sistema de Prevenção contra Intrusão para Segurança de Redes GX7800 da IBM

Avaliação Comparativa de Eficácia e Desempenho

Resumo Executivo

Atualmente, as redes corporativas enfrentam cada vez mais ameaças avançadas de um grande número de fontes, nunca antes visto. As soluções de proteção contra ameaças efetivas devem defender contra ameaças reais que estão evoluindo rapidamente e, ao mesmo tempo, proporcionar altos níveis de desempenho e disponibilidade. A IBM encarregou a Tolly para avaliar a sua rede com base em protocolo *Intrusion Prevention System* (IPS) GX7800 e comparar a sua eficácia, a partir de um dispositivo com base em Snort, uma plataforma com base em assinatura.

Os engenheiros da Tolly realizaram diferentes testes de desempenho com o GX7800 e alcançaram uma velocidade de transmissão de 35,7 Gbps sob cargas de tráfego combinado. Isto demonstra uma grande tolerância a sobrecargas da rede, crescimento e capacidade sobre as características de desempenho publicadas pela IBM. A Tolly também avaliou a eficácia e a funcionalidade do IBM IPS GX7800.

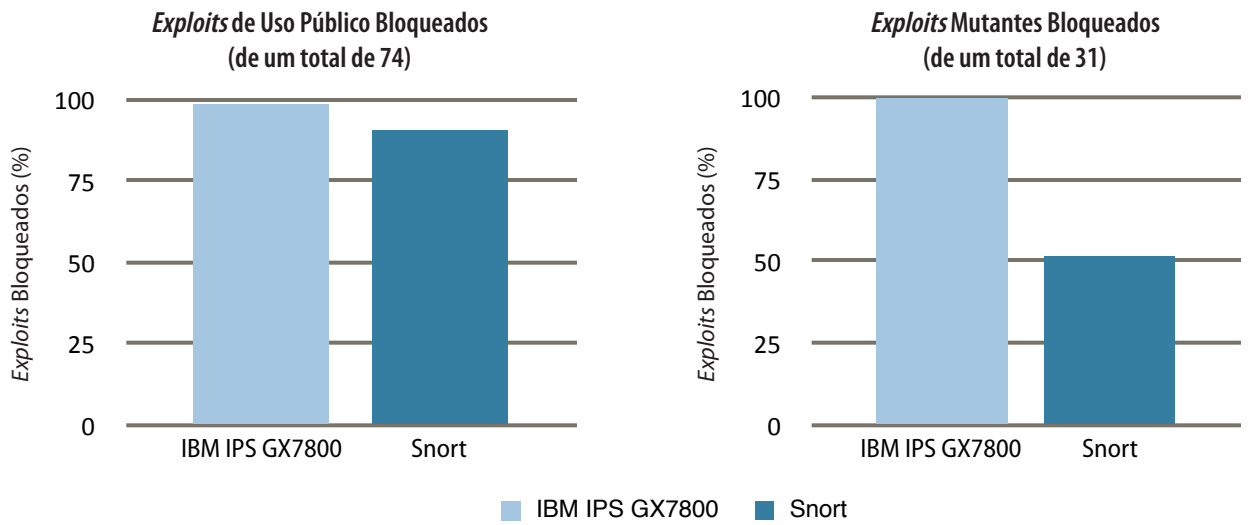
Os testes mostraram que o IBM IPS GX7800 é mais eficaz no bloqueio de *exploits* de uso público do que o Snort e, radicalmente mais eficaz ao bloquear *exploits* mutantes – bloqueando 100% em comparação aos 52% pelo Snort. Consulte a Figura 1.

Os Resultados

O IBM Network Security IPS GX7800:

1. Proporciona proteção superior a ameaças desenvolvidas com altos níveis de desempenho
2. Interrompeu 99% dos ataques de uso público testados
3. Foi quase duas vezes tão eficaz quanto o Snort, impedindo ataques mutantes
4. Protegeu fluxos de 100% de tráfego HTTP na velocidade de 20 Gbps e cargas de tráfego combinado de mais de 35 Gbps

Eficácia do Sistema IPS em Linha Contra *Exploits* Mutantes e de Uso Público (PA)
IBM IPS GX7800 versus Snort IPS



Fonte: Tolly, outubro de 2012

Figura 1

Como a TI corporativa evoluiu, a segurança de rede deve manter o mesmo ritmo. As ameaças atuais são mais refinadas, diversificadas e potencialmente mais prejudiciais do que nunca – e como resultado, requerem soluções novas e intuitivas para compensar seu impacto negativo.

As soluções IPS tradicionais com base em assinatura não protegem contra ameaças em evolução, que estão sempre presentes no ambiente corporativo atual. As soluções IPS com base em assinatura podem proteger contra um *exploit* uma vez que seja conhecido, mas oferece menor proteção contra ameaças mutantes.

Utilizando o seu módulo de análise do protocolo (PAM - protocol analysis module), o IBM GX7800 é capaz de decodificar o tráfego de aplicativo e identificar códigos maliciosos em qualquer forma, ajudando assim a manter uma rede mais segura do que somente com o IPS com base em assinatura. Além disso, o mecanismo é extensível e pode abranger mais do que apenas vulnerabilidades (p. ex., SQL injection e código shell). O IBM GX7800 é apenas parte da solução que a IBM oferece. Nos bastidores, a equipe X-Force de pesquisa e desenvolvimento da IBM proativamente procura por novas ameaças, incorporando esta percepção novamente ao dispositivo por meio de atualizações de software.

Resultados dos Testes

Resultados dos Testes de Eficácia

Ameaças de Uso Público Bloqueadas

O IBM X-Force coletou *exploits* do banco de dados X-Force, onde são publicadas todas as vulnerabilidades divulgadas e *exploits* de muitas fontes.

Engenheiros da Tolly testaram o IBM GX7800 e o dispositivo de software livre Snort contra uma recompilação de 74 dessas ameaças. O IBM GX7800 impediu 99% (73 de um total de 74) dos *exploits*, enquanto que o dispositivo de software livre Snort bloqueou somente 67 de 74.

Ameaças Mutantes Bloqueadas

Tal como o segmento de antivírus, a Internet é hospedeira de um número cada vez maior de ameaças.

Você pode pensar em soluções com base em assinatura como um sistema de reconhecimento da face e a mutação como uma máscara que faz "mutação" da face e pode confundir o sistema de reconhecimento da face.

Soluções com base em assinatura têm dificuldades em se manter no ritmo quando ameaças estão em mutação aos milhares. A fim de replicar essas mutações, engenheiros deliberadamente alteraram as cargas úteis dos *exploits* testados. Isto foi alcançado na maioria dos casos ao mudar o nome de uma variável única dentro do código do *exploit*.

O IBM GX7800 impediu 100% de ameaças mutantes, enquanto a solução Snort com base em assinatura impediu metade (16 de 31) dos *exploits* mutantes. Consulte a Figura 1.

Resultados dos Testes de Desempenho

No atual ambiente corporativo, segurança é indispensável. No entanto, desempenho é igualmente importante para grandes implementações. Organizações precisam manter-se online e seguras a velocidades de 10GbE múltiplas.

Engenheiros verificaram o desempenho do IBM GX7800 utilizando o BreakingPoint FireStorm da Ixia em ambos os modos "descartar" (drop) e "reenviar" (forward) em toda a gama de tamanhos de objeto que incluíam fluxos de tráfego de HTTP puro, bem como fluxos contendo misto de tipos de tráfego corporativo e central.

Os resultados do teste da Tolly mostram que o IBM GX7800 pode manter altos níveis de desempenho em ambos os modos "descartar" e "reenviar". Testar com o modo "descartar" ativado não permite nenhum tráfego além do que o dispositivo possa ler em um determinado momento, considerando que com o modo "reenviar" ativado, o tráfego em excesso é encaminhado à rede sem ter sido lido, mas é importante para a continuidade dos negócios.

Divisão IBM Security Systems

IPS GX7800

Avaliação de Desempenho e Eficácia

Tolly. Certified

Testado em outubro de 2012

Com objetos de 44K, o IBM GX7800 proporcionou mais de 19 Gbps no modo "descartar" e mais de 24 Gbps no modo "reenviar".

O IBM GX7800 proporcionou resultados idênticos em ambos os modos para os perfis de tráfego IPS Principal e IPS Corporativo, demonstrando uma velocidade de transmissão de 35,7 Gbps para todos os quatro cenários (descartar/reenviar IPS Principal e descartar/reenviar IPS Corporativo). Consulte a Figura 2.

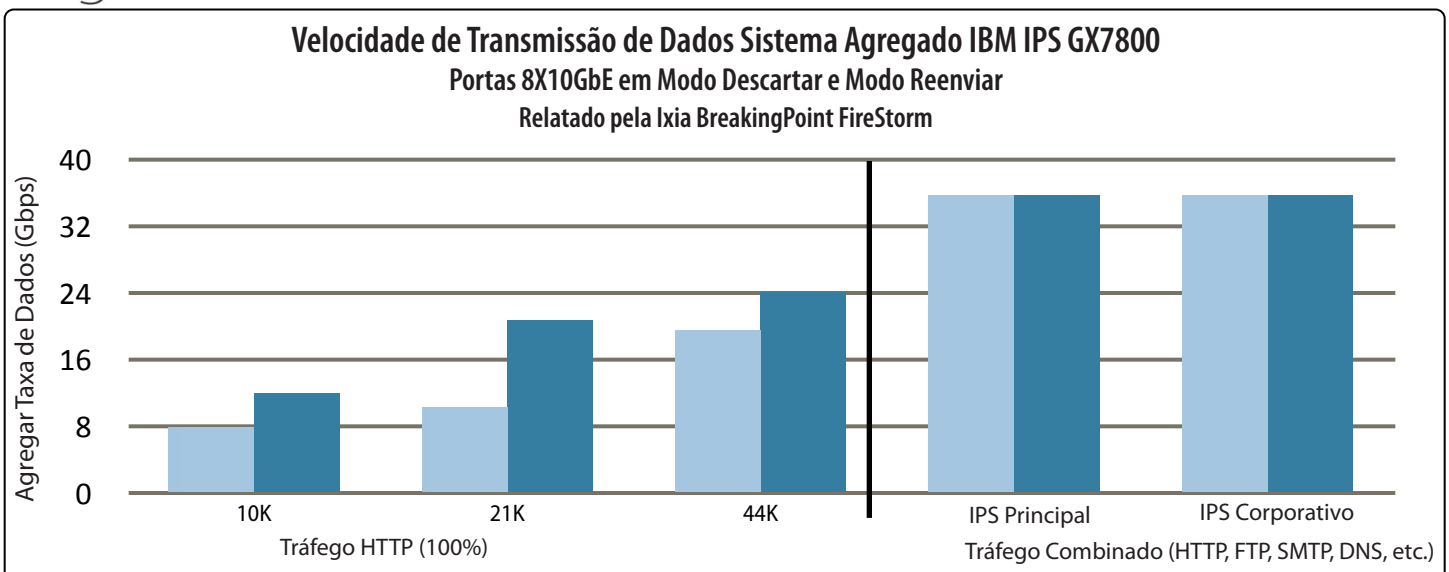
Recursos/Funcionalidade

Embora alguns recursos possam ser vistos como um extra, não se pode ignorar a utilidade de um sistema eficaz. O IBM GX7800 oferece uma variedade de recursos/funções que torna a sua implementação e gerenciamento intuitivo e fácil de utilizar.

Do painel, administradores são saudados com uma "visão rápida" para a segurança de rede global, incluindo eventos recentes e estatísticas gerais para muitos dos módulos e ameaças.

Por padrão, o IBM GX7800 é equipado com políticas poderosas em forma de X-Force Virtual Patch, uma coleção de algoritmos de proteção que são especificamente concebidos para não gerar falsos positivos e agir como um suporte para muitas correções de aplicativos.

[1] Snort® é um sistema (IDS/IPS) de detecção e prevenção de invasão em rede de software livre desenvolvido pela Sourcefire.



Fonte: Tolly, outubro de 2012 Figura 2

Além de fornecer segurança de alto desempenho, o GX7800 também hospeda uma matriz de outras funções incluindo um simples módulo Network Data Loss Prevention (NDLP) e proteção de aplicativo web. Estas inclusões transformam o GX7800 em um dispositivo de segurança de rede para várias finalidades. O GX-7800 também pode ser implementado em cenários de alta disponibilidade dentro de uma organização a fim de aumentar a quantidade de tráfego que pode ser inspecionado. Da mesma forma, dispositivos múltiplos podem ser implementados em locais geograficamente distintos dentro de uma organização. Nesta topologia, dispositivos compartilham informação entre si e podem ser geridos de forma centralizada a partir de um único console.

Configuração de Teste e Metodologia

Configuração do Laboratório de Teste

Engenheiros implementaram um ambiente que consistia em um IBM Network Security Intrusion Prevention System GX7800, que foi equipado com 8 portas de 10 GbE, executando firmware v4.5 com conteúdo de segurança XPU versão 32.090.

O teste foi realizado em um ambiente VMware ESXi 5.0.0. Múltiplos clientes foram implementados e configurados para serem vulneráveis aos *exploits* testados. O Snort foi implementado no cliente CentOS com 1 vCPU e 2GB de RAM. Múltiplas redes de MVs foram criadas dentro do host para diferenciar a rede "Invasora" da rede "Vulnerável".

A instância Snort foi definida com as atualizações mais recentes do VRT (Vulnerability Research Team) de 16 de outubro de 2012, e estava executando em Snort Engine versão 2.9.3.1, configurado em modo em linha. Para garantir que foram utilizadas as mais altas configurações de segurança, engenheiros definiram todos os Snort Rules e SO_Rules para "Bloquear" como padrão. Ambas as regras de texto simples e ofuscado, e as regras de objeto compartilhado foram utilizadas para o teste.

Soluções de Prevenção de Invasão para Segurança de Redes IBM Especificações do Produto

Características de Desempenho
- 200 Mbps a 20 Gbp + velocidade de transmissão agregada (dependendo do modelo)
- 1,3M a 21M de conexões simultâneas (dependendo do modelo)
- Menos de 150 microssegundos de latência (inferior a 75 microssegundos para os modelos GX7)

Capacidades Principais
- Tecnologia de Correção Virtual
- Proteção de Aplicativos da Web
- Proteção contra ataques no lado do cliente
- Segurança de dados e conteúdo
- Reconhecimento de aplicativos

Modos de Proteção
- Proteção em linha
- Simulação em linha
- Monitoramento passivo

Disponibilidade
- Alta disponibilidade ativa/ativa
- Unidades de disco rígido e fontes de alimentação redundantes

Pesquisa/Atualizações
- Atualizações proporcionadas pela equipe de pesquisa IBM X-Force
- Atualizações X-Press – entrega atualizada automatizada

Opções de Gerenciamento
- Gerenciamento com base na web local
- Gerenciamento centralizado via IBM Site Protector

Para mais informações, ligue 0800-707-1426 opção 4 (informe o código: SEGURANÇA), ou visite:
http://www.ibm.com/software/tivoli/products/security-network-intrusion-prevention/ **Fonte: IBM**

O Snort pede cobertura para todas as vulnerabilidades e exposições comuns (CVE – common vulnerabilities and exposures) utilizadas no teste.

Metodologia do Teste

Para testes de eficácia, o Metasploit Framework 4.5.0-dev-15713 foi utilizado para criar carga útil e entregar os *exploits* a host vulneráveis. Os *exploits* de uso público foram utilizados para todos os CVEs. "Mutantes" eram *exploits* com várias mudanças no código (como por exemplo, alteravam os nomes de variáveis/funções) que produziu o mesmo resultado que o *exploit* original. Trata-se de uma abordagem comum utilizada para atacar sistemas. Consulte a Figura 4.

Inicialmente, *exploits* foram executados sem nenhuma solução de segurança em linha e captura de pacotes foi criada para ambos os lados da conversação.

O Idappcom Traffic IQ Professional v2.0.299 foi utilizado para reproduzir ambos os lados da conversação por meio de interfaces nas redes vulneráveis e do invasor enquanto cada dispositivo IPS foi conectado em modo em linha. O Traffic IQ foi configurado para reescrever os cabeçalhos HTTP, com um tempo de atraso de 2 segundos entre reproduções de rastreamento.

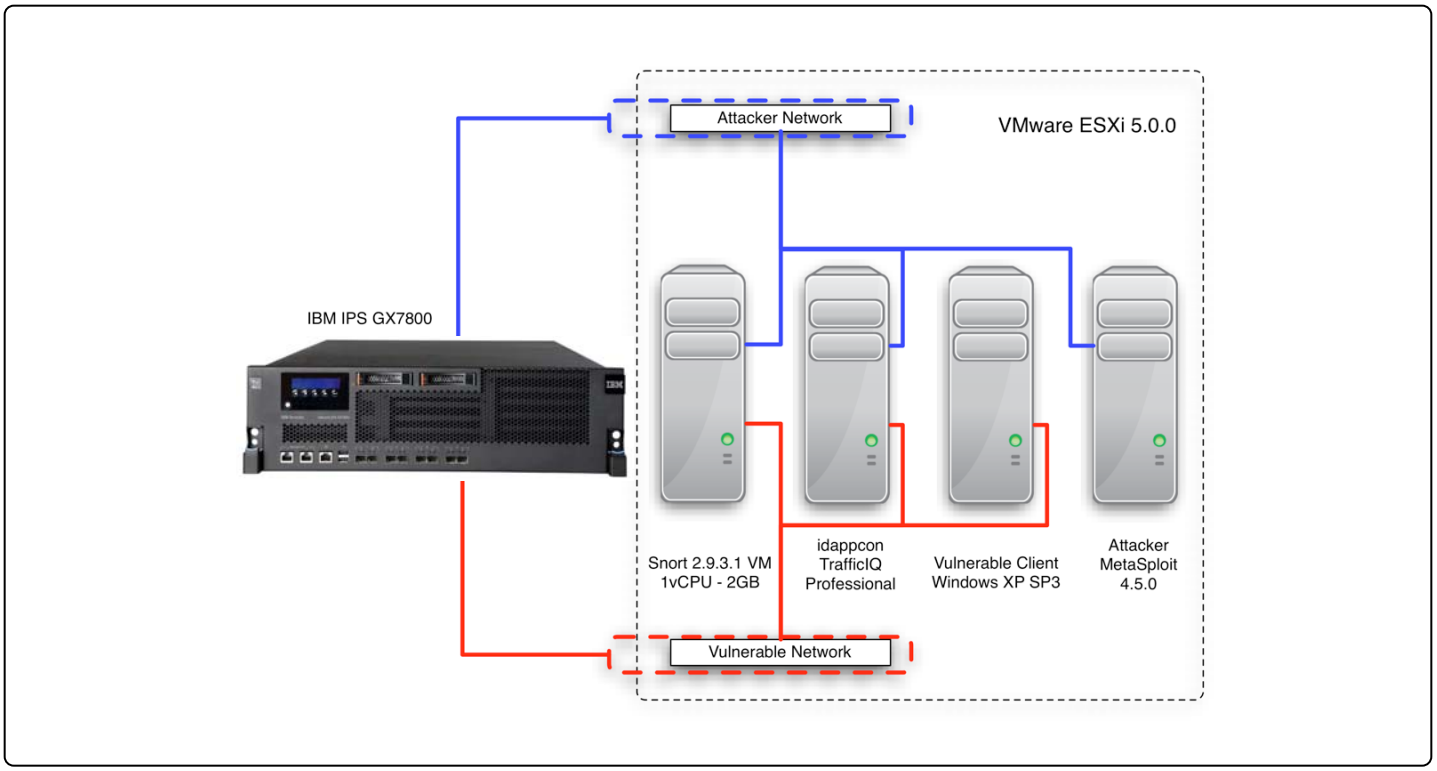
Todos os 74 *exploits* de base e as 31 mutações foram executados por meio de ambiente e resultados reproduzíveis foram relatados pelo Traffic IQ.

Para os testes de Desempenho, a Tolly utilizou um sistema Ixia BreakingPoint FireStorm versão 3.0 b105019. Engenheiros testaram três tamanhos de objetos HTTP (10K, 21K e 44K) com 250 clientes/servidores por perfil de AppSim, com dois em cada porta para obter transações bidirecionais. Além disso, engenheiros utilizaram os tráfegos combinados IPS Principal e Corporativo para realçar o GX7800. Estas combinações continham HTTP, SMTP, SIP, FTP, DNS e outros tráfegos com monitoração de estado.

Os testes foram executados em 5 minutos e ambos os modos Descartar e Reenviar definido no IBM GX7800. Devido à natureza do tráfego BreakingPoint, certos ataques DOS ocasionalmente poderiam disparar durante a realização dos testes. Para efeitos de testes de desempenho, estas regras foram desativadas para permitir o fluxo de tráfego sem erros.

Engenheiros também injetaram um StrikePack de 6 ataques para verificar que os ataques estavam sendo detectados em situação de carga pesada. Em nenhum cenário foram permitidos ataques por meio do GX7800.

Fornecedor	Produto	Web
Ixia	Ixia BreakingPoint FireStorm V3.0	IXIA TESTED http://www.ixiacom.com



Dados do Teste: Exemplos de Mutação e Vulnerabilidades **Comuns**

Exemplo de Mutação 1: Renomeando Variáveis
Muitos dos *exploits* testados contêm nomes variáveis. Estes nomes variáveis são irrelevantes para a exploração bem-sucedida e, portanto, não pode ser um método confiável para detecção de tentativas de *exploits*. A fim de testar versões mutantes dos *exploits*, simplesmente alteramos os nomes variáveis, como mostrado nos exemplos abaixo:

Nomes das variáveis originais	Nomes das variáveis mutantes
Shellcode	somecode
Block	brick
heapLib	badLib

Enquanto estas mudanças não tiveram impacto na eficácia dos *exploits*, elas permitiram que os *exploits* passassem despercebidos pela solução Snort com base em assinatura.

Exemplo de Mutação 2: Renomeando as Referências de Classe
Muitos dos *exploits* testados contêm referências a classes contidas em arquivos Java. Pelo fato dos nomes dos arquivos de classe em um archive serem variáveis e arbitrários, eles devem ser confiáveis para detecção de atividades maliciosas. A fim de testar versões mutantes dos *exploits*, simplesmente alteramos os nomes das classes referenciadas, como mostrado no exemplo abaixo:

Referência da Classe Original	Referência da Classe Mutante
<html><head></head> <body><applet archive="jmBXTMuv.jar" code="msf.x.Exploit.class" width="1" height="1"xparam name="data" value=""/xparam name="iar">	<html><headx/head> <bodyxapplet archive="eXRZLr.jar" code="msf.x.badguy.class" width="1" height="1"xparam name="data" value=""/xparam name="iar">

Enquanto estas mudanças não tiveram impacto na eficácia dos *exploits*, elas permitiram que os *exploits* passassem despercebidos pela solução Snort com base em assinatura.

Exemplo de Mutação 3: Adicionando Comentários
A fim de testar versões mutantes de alguns dos *exploits*, simplesmente adicionamos comentários ao código do *exploit*, como mostrado no exemplo abaixo:

Código Original	Código Mutante
var t = unescape;	var t = unescape <!— Comment -->;

Enquanto estas mudanças não tiveram nenhum impacto na eficácia dos *exploits*, eles permitiram que os *exploits* passassem despercebidos pela solução Snort com base em assinatura.

Vulnerabilidades dos Servidores Testados

CVE-2012-0002	CVE-2011-4191	CVE-2011-3192	CVE-2011-1248	CVE-2011-1206
CVE-2011-0807	CVE-2011-0654	CVE-2011-0267	CVE-2011-0266	CVE-2010-3972
CVE-2010-2729	CVE-2010-1555	CVE-2010-0478	CVE-2009-3103	CVE-2009-3023
CVE-2009-1429	CVE-2008-4250	CVE-2008-1697		

Vulnerabilidades dos Clientes Testados

CVE-2012-1889	CVE-2012-1875	CVE-2012-0779	CVE-2012-0507	CVE-2012-0500
CVE-2012-0158	CVE-2012-0013	CVE-2011-3544	CVE-2011-3400	CVE-2011-2462
CVE-2011-1260	CVE-2011-0611	CVE-2011-0609	CVE-2011-0105	CVE-2011-0073
CVE-2011-0065	CVE-2011-0041	CVE-2011-0027	CVE-2010-4452	CVE-2010-3971
CVE-2010-3970	CVE-2010-3962	CVE-2010-3654	CVE-2010-3653	CVE-2010-3552
CVE-2010-3333	CVE-2010-3148	CVE-2010-2883	CVE-2010-2568	CVE-2010-1885
CVE-2010-1423	CVE-2010-1297	CVE-2010-1240 X2	CVE-2010-0842	CVE-2010-0840
CVE-2010-0806	CVE-2010-0805	CVE-2010-0249	CVE-2010-0248	CVE-2010-0188
CVE-2010-0094	CVE-2010-0033	CVE-2010-0027	CVE-2009-4324	CVE-2009-3459
CVE-2009-2477	CVE-2009-1534	CVE-2009-1136	CVE-2009-0927	CVE-2009-0658
CVE-2009-0075	CVE-2008-4844	CVE-2008-4037	CVE-2008-2992	CVE-2008-0015

Nota: Para visualizar detalhes de um determinado CVE, utilize o seguinte formato com o nome do CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1206
Fonte: Tolly, outubro de 2012

Figura 4

Sobre a Tolly

As empresas Tolly Group têm proporcionado serviços de TI de nível mundial por mais de 20 anos. A Tolly é uma provedora de liderança global em serviços terceirizados de validação para fornecedores de produtos, componentes e serviços de TI.

Você pode entrar em contato com a empresa pelo email sales@tolly.com, ou pelo telefone +1 561.391.5610.

Visite o site da Tolly em:
http://www.tolly.com

Interação com os Concorrentes

De acordo com o *Fair Testing Charter da Tolly*, a equipe da Tolly convidou representantes da Sourcefire, Inc., desenvolvedor do Snort, para participar do teste. A Sourcefire examinou o plano de teste e recusou-se a participar.

Para mais informações sobre a *Tolly Fair Testing Charter*, visite:
http://www.tolly.com/FTC.aspx

Termos de Utilização

Este documento é fornecido gratuitamente para ajudá-lo a entender se um determinado produto, tecnologia ou serviço merecem investigação adicional para as suas necessidades particulares. Qualquer decisão de compra de um produto deve ser feita com base em sua própria avaliação de adequação com base em suas necessidades. O documento nunca deve ser utilizado como um substituto para aconselhamento de um profissional qualificado de TI ou negócios. Esta avaliação deu ênfase a ilustrar recursos específicos e/ou desempenho do(s) produto(s) e foi conduzida sob condições controladas de laboratório. Certos testes podem ter sido adaptados para refletir desempenho sob condições ideais; o desempenho pode variar sob condições reais. Os usuários devem executar testes com base em seu cenário real próprio para validar o desempenho para as suas redes próprias.

Esforços razoáveis foram feitos para garantir a exatidão dos dados aqui contidos, mas erros e/ou omissões podem ocorrer. O teste/auditoria aqui documentado também pode depender de diversas ferramentas de testes cuja precisão está fora do nosso controle. Além disso, o documento depende de determinadas representações do patrocinador, que está além do nosso controle verificar. Dentre estes é que o software/hardware testado é de produção ou de produção rastreada e está, ou estará, disponível em forma equivalente, ou melhor, aos clientes comerciais. Assim, este documento é fornecido "no estado em que se encontra", e a Tolly Enterprises, LLC (Tolly) não oferece garantia, representação ou obrigação, seja expressa ou implícita, e não aceita qualquer responsabilidade jurídica, seja direta ou indireta, para a precisão, integralidade, utilidade ou adequação de nenhuma informação aqui contida. Ao revisar este documento, você concorda que a sua utilização de qualquer informação aqui contida é de seu próprio risco, e você aceita todos os riscos e responsabilidades por perdas, danos, custos e outras consequências resultantes, direta ou indiretamente, de qualquer informação ou material disponível no mesmo. A Tolly não se responsabiliza por, e você concorda em manter a Tolly e suas afiliadas relacionadas isentas de qualquer perda, prejuízo, acidente ou dano resultantes de ou decorrentes da sua utilização ou na dependência de qualquer informação aqui prestada.

A Tolly não faz nenhuma declaração em relação a qualquer produto ou empresa aqui descrito, se é adequado para o investimento. Você deve obter conselho do seu próprio profissional independente, seja jurídico, contábil ou qualquer outro, antes de prosseguir com qualquer investimento ou projeto relacionado a qualquer informação, produtos ou empresas aqui descritas. Quando existem traduções a outros idiomas, o documento em Inglês é considerado o válido. Para garantir precisão, utilize apenas documentos baixados diretamente de Tolly.com. Nenhuma parte de qualquer documento deve ser reproduzida, no todo ou em parte, sem a permissão por escrito específica da Tolly. Todas as marcas registradas utilizadas no documento são de propriedade de seus respectivos proprietários. Você concorda em não utilizar qualquer marca registrada em ou como totalidade ou parte das suas próprias marcas em conexão com quaisquer atividades, produtos ou serviços que não sejam nossos, ou de uma forma que possa ser confusa, enganosa ou ilusória ou de uma forma que deprecia a nós ou a nossa informação, projetos e empreendimentos.

212148 jwft1 jt-mts-wt-2012-11-29-VerO